aws

リファレンスガイド

AWS 管理ポリシー

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS 管理ポリシー: リファレンスガイド

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon の商標およびトレードドレスは Amazon 以外の製品およびサービスに使用することはできません。また、お客様に誤解を与える可能性がある形式で、または Amazon の信用を損なう形式で使用することもできません。Amazon が所有していないその他のすべての商標は Amazon との提携、関連、支援関係の有無にかかわらず、それら該当する所有者の資産です。

Table of Contents

AWS マネージドポリシーとは何ですか? 1
ポリシーリファレンスページについて 1
非推奨の AWS マネージドポリシー 2
AWS マネージドポリシー 3
AccessAnalyzerServiceRolePolicy 52
このポリシーを使用すると 52
ポリシーの詳細 52
ポリシーのバージョン 52
JSON ポリシードキュメント 53
詳細はこちら 55
AccountManagementFromVercel 55
このポリシーを使用すると 56
ポリシーの詳細 56
ポリシーのバージョン 56
JSON ポリシードキュメント 56
詳細はこちら 57
AdministratorAccess 57
このポリシーを使用すると 57
ポリシーの詳細 57
ポリシーのバージョン 58
JSON ポリシードキュメント 58
詳細はこちら 58
AdministratorAccess-Amplify 58
このポリシーを使用すると 58
ポリシーの詳細 59
ポリシーのバージョン 59
JSON ポリシードキュメント 59
詳細はこちら 69
AdministratorAccess-AWSElasticBeanstalk 70
このポリシーを使用すると 70
ポリシーの詳細 70
ポリシーのバージョン 70
JSON ポリシードキュメント 70
詳細はこちら 78

AIOpsAssistantIncidentReportPolicy 79
このポリシーを使用すると 79
ポリシーの詳細 79
ポリシーのバージョン 79
JSON ポリシードキュメント 79
詳細はこちら 80
AIOpsAssistantPolicy 80
このポリシーを使用すると 81
ポリシーの詳細 81
ポリシーのバージョン 81
JSON ポリシードキュメント 81
詳細はこちら 102
AIOpsConsoleAdminPolicy 102
このポリシーを使用すると 102
ポリシーの詳細 102
ポリシーのバージョン 102
JSON ポリシードキュメント 103
詳細はこちら 109
AIOpsOperatorAccess 109
このポリシーを使用すると 109
ポリシーの詳細 109
ポリシーのバージョン 109
JSON ポリシードキュメント 109
詳細はこちら 112
AIOpsReadOnlyAccess 113
このポリシーを使用すると 113
ポリシーの詳細 113
ポリシーのバージョン 113
JSON ポリシードキュメント 113
詳細はこちら 114
AlexaForBusinessDeviceSetup 114
このポリシーを使用すると 114
ポリシーの詳細 114
ポリシーのバージョン 115
JSON ポリシードキュメント 115
詳細はこちら 115

AlexaForBusinessFullAccess 116
このポリシーを使用すると 116
ポリシーの詳細 116
ポリシーのバージョン 116
JSON ポリシードキュメント 116
詳細はこちら 118
AlexaForBusinessGatewayExecution 118
このポリシーを使用すると 118
ポリシーの詳細 118
ポリシーのバージョン 118
JSON ポリシードキュメント 119
詳細はこちら 119
AlexaForBusinessLifesizeDelegatedAccessPolicy 120
このポリシーを使用すると 120
ポリシーの詳細 120
ポリシーのバージョン 120
JSON ポリシードキュメント 120
詳細はこちら 123
AlexaForBusinessNetworkProfileServicePolicy 123
このポリシーを使用すると 123
ポリシーの詳細 123
ポリシーのバージョン 123
JSON ポリシードキュメント 124
詳細はこちら 124
AlexaForBusinessPolyDelegatedAccessPolicy 124
このポリシーを使用すると 125
ポリシーの詳細 125
ポリシーのバージョン 125
JSON ポリシードキュメント 125
詳細はこちら 127
AlexaForBusinessReadOnlyAccess 127
このポリシーを使用すると 127
ポリシーの詳細 127
ポリシーのバージョン 127
JSON ポリシードキュメント 128
詳細はこちら 128

AmazonAPIGatewayAdministrator 128
このポリシーを使用すると 128
ポリシーの詳細 129
ポリシーのバージョン 129
JSON ポリシードキュメント 129
詳細はこちら 129
AmazonAPIGatewayInvokeFullAccess 130
このポリシーを使用すると 130
ポリシーの詳細 130
ポリシーのバージョン 130
JSON ポリシードキュメント 130
詳細はこちら 131
AmazonAPIGatewayPushToCloudWatchLogs 131
このポリシーを使用すると 131
ポリシーの詳細 131
ポリシーのバージョン 131
JSON ポリシードキュメント 132
詳細はこちら 132
AmazonAppFlowFullAccess 132
このポリシーを使用すると 132
ポリシーの詳細 133
ポリシーのバージョン 133
JSON ポリシードキュメント 133
詳細はこちら 136
AmazonAppFlowReadOnlyAccess 136
このポリシーを使用すると 136
ポリシーの詳細 136
ポリシーのバージョン 136
JSON ポリシードキュメント 137
詳細はこちら 137
AmazonApplicationRecoveryControllerRegionSwitchPlanExecutionPolicy 137
このポリシーを使用すると 138
ポリシーの詳細 138
ポリシーのバージョン 138
JSON ポリシードキュメント 138
詳細はこちら 139

AmazonAppStreamFullAccess 139
このポリシーを使用すると 139
ポリシーの詳細 139
ポリシーのバージョン 140
JSON ポリシードキュメント 140
詳細はこちら 142
AmazonAppStreamPCAAccess 142
このポリシーを使用すると 142
ポリシーの詳細 142
ポリシーのバージョン 142
JSON ポリシードキュメント 142
詳細はこちら 143
AmazonAppStreamReadOnlyAccess 143
このポリシーを使用すると 143
ポリシーの詳細 143
ポリシーのバージョン 144
JSON ポリシードキュメント 144
詳細はこちら 144
AmazonAppStreamServiceAccess 144
このポリシーを使用すると 145
ポリシーの詳細 145
ポリシーのバージョン 145
JSON ポリシードキュメント 145
詳細はこちら 146
AmazonAthenaFullAccess 146
このポリシーを使用すると 147
ポリシーの詳細 147
ポリシーのバージョン 147
JSON ポリシードキュメント 147
詳細はこちら 151
AmazonAthenaServiceRolePolicy 151
このポリシーを使用すると 151
ポリシーの詳細 151
ポリシーのバージョン 151
JSON ポリシードキュメント 152
詳細はこちら 152

AmazonAugmentedAIFullAccess 152
このポリシーを使用すると 152
ポリシーの詳細 153
ポリシーのバージョン 153
JSON ポリシードキュメント 153
詳細はこちら 154
AmazonAugmentedAIHumanLoopFullAccess 154
このポリシーを使用すると 154
ポリシーの詳細 154
ポリシーのバージョン 155
JSON ポリシードキュメント 155
詳細はこちら 155
AmazonAugmentedAIIntegratedAPIAccess 156
このポリシーを使用すると 156
ポリシーの詳細 156
ポリシーのバージョン 156
JSON ポリシードキュメント 156
詳細はこちら 158
AmazonAuroraDSQLConsoleFullAccess 158
このポリシーを使用すると 158
ポリシーの詳細 158
ポリシーのバージョン 158
JSON ポリシードキュメント 158
詳細はこちら 160
AmazonAuroraDSQLFullAccess 161
このポリシーを使用すると 161
ポリシーの詳細 161
ポリシーのバージョン 161
JSON ポリシードキュメント 161
詳細はこちら 164
AmazonAuroraDSQLReadOnlyAccess 164
このポリシーを使用すると 164
ポリシーの詳細 164
ポリシーのバージョン 164
JSON ポリシードキュメント 164
詳細はこちら 165

AmazonBedrockAgentCoreMemoryBedrockModelInferenceExecutionRolePolicy 165
このポリシーを使用すると 166
ポリシーの詳細 166
ポリシーのバージョン 166
JSON ポリシードキュメント 166
詳細はこちら 167
AmazonBedrockFullAccess 167
このポリシーを使用すると 167
ポリシーの詳細 167
ポリシーのバージョン 167
JSON ポリシードキュメント 168
詳細はこちら 173
AmazonBedrockLimitedAccess 173
このポリシーを使用すると 173
ポリシーの詳細 173
ポリシーのバージョン 173
JSON ポリシードキュメント 174
詳細はこちら 176
AmazonBedrockMantleFullAccess 176
このポリシーを使用すると 176
ポリシーの詳細 176
ポリシーのバージョン 176
JSON ポリシードキュメント 177
詳細はこちら 177
AmazonBedrockMantleInferenceAccess 177
このポリシーを使用すると 177
ポリシーの詳細 178
ポリシーのバージョン 178
JSON ポリシードキュメント 178
詳細はこちら 179
AmazonBedrockMantleReadOnly 179
このポリシーを使用すると 179
ポリシーの詳細 179
ポリシーのバージョン 179
JSON ポリシードキュメント 179
詳細はこちら 180

AmazonBedrockMarketplaceAccess 180
このポリシーを使用すると 180
ポリシーの詳細 180
ポリシーのバージョン 181
JSON ポリシードキュメント 181
詳細はこちら 185
AmazonBedrockReadOnly 185
このポリシーを使用すると 186
ポリシーの詳細 186
ポリシーのバージョン 186
JSON ポリシードキュメント 186
詳細はこちら 187
AmazonBedrockStudioPermissionsBoundary 188
このポリシーを使用すると 188
ポリシーの詳細 188
ポリシーのバージョン 188
JSON ポリシードキュメント 188
詳細はこちら 192
AmazonBraketFullAccess 193
このポリシーを使用すると 193
ポリシーの詳細 193
ポリシーのバージョン 193
JSON ポリシードキュメント 193
詳細はこちら 197
AmazonBraketJobsExecutionPolicy 198
このポリシーを使用すると 198
ポリシーの詳細 198
ポリシーのバージョン 198
JSON ポリシードキュメント 198
詳細はこちら 201
AmazonBraketServiceRolePolicy 201
このポリシーを使用すると 201
ポリシーの詳細 201
ポリシーのバージョン 202
JSON ポリシードキュメント 202
詳細はこちら 203

AmazonChimeFullAccess 203
このポリシーを使用すると 203
ポリシーの詳細 203
ポリシーのバージョン 203
JSON ポリシードキュメント 203
詳細はこちら 206
AmazonChimeReadOnly 206
このポリシーを使用すると 206
ポリシーの詳細 206
ポリシーのバージョン 206
JSON ポリシードキュメント 206
詳細はこちら 207
AmazonChimeSDK 207
このポリシーを使用すると 207
ポリシーの詳細 207
ポリシーのバージョン 208
JSON ポリシードキュメント 208
詳細はこちら 209
AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy 209
このポリシーを使用すると 209
ポリシーの詳細 209
ポリシーのバージョン 210
JSON ポリシードキュメント 210
詳細はこちら 211
AmazonChimeSDKMessagingServiceRolePolicy 211
このポリシーを使用すると 211
ポリシーの詳細 211
ポリシーのバージョン 212
JSON ポリシードキュメント 212
詳細はこちら 213
AmazonChimeServiceRolePolicy 213
このポリシーを使用すると 213
ポリシーの詳細 213
ポリシーのバージョン 213
JSON ポリシードキュメント 214
詳細はこちら 214

AmazonChimeTranscriptionServiceLinkedRolePolicy 214
このポリシーを使用すると 214
ポリシーの詳細 215
ポリシーのバージョン 215
JSON ポリシードキュメント 215
詳細はこちら 215
AmazonChimeUserManagement 216
このポリシーを使用すると 216
ポリシーの詳細 216
ポリシーのバージョン 216
JSON ポリシードキュメント 216
詳細はこちら 217
AmazonChimeVoiceConnectorServiceLinkedRolePolicy 218
このポリシーを使用すると 218
ポリシーの詳細 218
ポリシーのバージョン 218
JSON ポリシードキュメント 218
詳細はこちら 220
AmazonCloudDirectoryFullAccess 220
このポリシーを使用すると 220
ポリシーの詳細 221
ポリシーのバージョン 221
JSON ポリシードキュメント 221
詳細はこちら 221
AmazonCloudDirectoryReadOnlyAccess 222
このポリシーを使用すると 222
ポリシーの詳細 222
ポリシーのバージョン 222
JSON ポリシードキュメント 222
詳細はこちら 223
AmazonCloudWatchEvidentlyFullAccess 223
このポリシーを使用すると 223
ポリシーの詳細 223
ポリシーのバージョン 223
JSON ポリシードキュメント 224
詳細はこちら 226

AmazonCloudWatchEvidentlyReadOnlyAccess 226
このポリシーを使用すると 226
ポリシーの詳細 227
ポリシーのバージョン 227
JSON ポリシードキュメント 227
詳細はこちら 227
AmazonCloudWatchEvidentlyServiceRolePolicy 228
このポリシーを使用すると 228
ポリシーの詳細 228
ポリシーのバージョン 228
JSON ポリシードキュメント 228
詳細はこちら 230
AmazonCloudWatchRUMFullAccess 230
このポリシーを使用すると 230
ポリシーの詳細 230
ポリシーのバージョン 230
JSON ポリシードキュメント 231
詳細はこちら 233
AmazonCloudWatchRUMReadOnlyAccess 233
このポリシーを使用すると 233
ポリシーの詳細 234
ポリシーのバージョン 234
JSON ポリシードキュメント 234
詳細はこちら 235
AmazonCloudWatchRUMServiceRolePolicy 236
このポリシーを使用すると 236
ポリシーの詳細 236
ポリシーのバージョン 236
JSON ポリシードキュメント 236
詳細はこちら 237
AmazonCodeCatalystFullAccess 237
このポリシーを使用すると 237
ポリシーの詳細 237
ポリシーのバージョン 238
JSON ポリシードキュメント 238
詳細はこちら 239

AmazonCodeCatalystReadOnlyAccess 239
このポリシーを使用すると 239
ポリシーの詳細 239
ポリシーのバージョン 239
JSON ポリシードキュメント 240
詳細はこちら 240
AmazonCodeCatalystSupportAccess 240
このポリシーを使用すると 240
ポリシーの詳細 240
ポリシーのバージョン 241
JSON ポリシードキュメント 241
詳細はこちら 242
AmazonCodeGuruProfilerAgentAccess 242
このポリシーを使用すると 242
ポリシーの詳細 242
ポリシーのバージョン 242
JSON ポリシードキュメント 242
詳細はこちら 243
AmazonCodeGuruProfilerFullAccess 243
このポリシーを使用すると 243
ポリシーの詳細 243
ポリシーのバージョン 244
JSON ポリシードキュメント 244
詳細はこちら 244
AmazonCodeGuruProfilerReadOnlyAccess 245
このポリシーを使用すると 245
ポリシーの詳細 245
ポリシーのバージョン 245
JSON ポリシードキュメント 245
詳細はこちら 246
AmazonCodeGuruReviewerFullAccess 246
このポリシーを使用すると 246
ポリシーの詳細 246
ポリシーのバージョン 247
JSON ポリシードキュメント 247
詳細はこちら 249

AmazonCodeGuruReviewerReadOnlyAccess 249
このポリシーを使用すると 250
ポリシーの詳細 250
ポリシーのバージョン 250
JSON ポリシードキュメント 250
詳細はこちら 251
AmazonCodeGuruReviewerServiceRolePolicy 251
このポリシーを使用すると 251
ポリシーの詳細 251
ポリシーのバージョン 251
JSON ポリシードキュメント 252
詳細はこちら 254
AmazonCodeGuruSecurityFullAccess 254
このポリシーを使用すると 254
ポリシーの詳細 254
ポリシーのバージョン 254
JSON ポリシードキュメント 254
詳細はこちら 255
AmazonCodeGuruSecurityScanAccess 255
このポリシーを使用すると 255
ポリシーの詳細 255
ポリシーのバージョン 255
JSON ポリシードキュメント 256
詳細はこちら 256
AmazonCognitoDeveloperAuthenticatedIdentities 256
このポリシーを使用すると 257
ポリシーの詳細 257
ポリシーのバージョン 257
JSON ポリシードキュメント 257
詳細はこちら 258
AmazonCognitoIdpEmailServiceRolePolicy 258
このポリシーを使用すると 258
ポリシーの詳細 258
ポリシーのバージョン 258
JSON ポリシードキュメント 259
詳細はこちら 259

AmazonCognitoIdpServiceRolePolicy 259
このポリシーを使用すると 259
ポリシーの詳細 260
ポリシーのバージョン 260
JSON ポリシードキュメント 260
詳細はこちら 260
AmazonCognitoPowerUser 261
このポリシーを使用すると 261
ポリシーの詳細 261
ポリシーのバージョン 261
JSON ポリシードキュメント 261
詳細はこちら 263
AmazonCognitoReadOnly 263
このポリシーを使用すると 263
ポリシーの詳細 263
ポリシーのバージョン 263
JSON ポリシードキュメント 263
詳細はこちら 264
AmazonCognitoUnAuthedIdentitiesSessionPolicy 264
このポリシーを使用すると 265
ポリシーの詳細 265
ポリシーのバージョン 265
JSON ポリシードキュメント 265
詳細はこちら 266
AmazonCognitoUnauthenticatedIdentities 266
このポリシーを使用すると 267
ポリシーの詳細 267
ポリシーのバージョン 267
JSON ポリシードキュメント 267
詳細はこちら 267
AmazonConnect_FullAccess 268
このポリシーを使用すると 268
ポリシーの詳細 268
ポリシーのバージョン 268
JSON ポリシードキュメント 268
詳細はこちら 271

AmazonConnectCampaignsServiceLinkedRolePolicy 271
このポリシーを使用すると 271
ポリシーの詳細 271
ポリシーのバージョン 272
JSON ポリシードキュメント 272
詳細はこちら 274
AmazonConnectReadOnlyAccess 274
このポリシーを使用すると 274
ポリシーの詳細 274
ポリシーのバージョン 274
JSON ポリシードキュメント 275
詳細はこちら 275
AmazonConnectServiceLinkedRolePolicy 275
このポリシーを使用すると 276
ポリシーの詳細 276
ポリシーのバージョン 276
JSON ポリシードキュメント 276
詳細はこちら 289
AmazonConnectSynchronizationServiceRolePolicy 289
このポリシーを使用すると 289
ポリシーの詳細 289
ポリシーのバージョン 289
JSON ポリシードキュメント 290
詳細はこちら 291
AmazonConnectVoiceIDFullAccess 292
このポリシーを使用すると 292
ポリシーの詳細 292
ポリシーのバージョン 292
JSON ポリシードキュメント 292
詳細はこちら 293
AmazonDataZoneBedrockModelConsumptionPolicy 293
このポリシーを使用すると 293
ポリシーの詳細 293
ポリシーのバージョン 293
JSON ポリシードキュメント 294
詳細はこちら 296

AmazonDataZoneBedrockModelManagementPolicy 296
このポリシーを使用すると 296
ポリシーの詳細 296
ポリシーのバージョン 297
JSON ポリシードキュメント 297
詳細はこちら 299
AmazonDataZoneDomainExecutionRolePolicy 299
このポリシーを使用すると 299
ポリシーの詳細 299
ポリシーのバージョン 299
JSON ポリシードキュメント 300
詳細はこちら 303
AmazonDataZoneEnvironmentRolePermissionsBoundary 303
このポリシーを使用すると 303
ポリシーの詳細 304
ポリシーのバージョン 304
JSON ポリシードキュメント 304
詳細はこちら 317
AmazonDataZoneFullAccess 317
このポリシーを使用すると 317
ポリシーの詳細 317
ポリシーのバージョン 317
JSON ポリシードキュメント 318
詳細はこちら 327
AmazonDataZoneFullUserAccess 327
このポリシーを使用すると 327
ポリシーの詳細 327
ポリシーのバージョン 327
JSON ポリシードキュメント 327
詳細はこちら 331
AmazonDataZoneGlueManageAccessRolePolicy 331
このポリシーを使用すると 331
ポリシーの詳細 331
ポリシーのバージョン 332
JSON ポリシードキュメント 332
詳細はこちら 340

AmazonDataZonePortalFullAccessPolicy 340
このポリシーを使用すると 340
ポリシーの詳細 340
ポリシーのバージョン 340
JSON ポリシードキュメント 340
詳細はこちら 341
AmazonDataZonePreviewConsoleFullAccess 341
このポリシーを使用すると 341
ポリシーの詳細 341
ポリシーのバージョン 341
JSON ポリシードキュメント 342
詳細はこちら 343
AmazonDataZoneProjectDeploymentPermissionsBoundary 344
このポリシーを使用すると 344
ポリシーの詳細 344
ポリシーのバージョン 344
JSON ポリシードキュメント 344
詳細はこちら 352
AmazonDataZoneProjectRolePermissionsBoundary 353
このポリシーを使用すると 353
ポリシーの詳細 353
ポリシーのバージョン 353
JSON ポリシードキュメント 353
詳細はこちら 360
AmazonDataZoneRedshiftGlueProvisioningPolicy 361
このポリシーを使用すると 361
ポリシーの詳細 361
ポリシーのバージョン 361
JSON ポリシードキュメント 361
詳細はこちら 369
AmazonDataZoneRedshiftManageAccessRolePolicy 369
このポリシーを使用すると 369
ポリシーの詳細 370
ポリシーのバージョン 370
JSON ポリシードキュメント 370
詳細はこちら 373

AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary 373
このポリシーを使用すると 374
ポリシーの詳細 374
ポリシーのバージョン 374
JSON ポリシードキュメント 374
詳細はこちら 401
AmazonDataZoneSageMakerManageAccessRolePolicy 402
このポリシーを使用すると 402
ポリシーの詳細 402
ポリシーのバージョン 402
JSON ポリシードキュメント 402
詳細はこちら 407
AmazonDataZoneSageMakerProvisioningRolePolicy 407
このポリシーを使用すると 407
ポリシーの詳細 407
ポリシーのバージョン 408
JSON ポリシードキュメント 408
詳細はこちら 412
AmazonDetectiveFullAccess 413
このポリシーを使用すると 413
ポリシーの詳細 413
ポリシーのバージョン 413
JSON ポリシードキュメント 413
詳細はこちら 414
AmazonDetectiveInvestigatorAccess 415
このポリシーを使用すると 415
ポリシーの詳細 415
ポリシーのバージョン 415
JSON ポリシードキュメント 415
詳細はこちら 417
AmazonDetectiveMemberAccess 417
このポリシーを使用すると 417
ポリシーの詳細 417
ポリシーのバージョン 417
JSON ポリシードキュメント 418
詳細はこちら 418

AmazonDetectiveOrganizationsAccess 418
このポリシーを使用すると 419
ポリシーの詳細 419
ポリシーのバージョン 419
JSON ポリシードキュメント 419
詳細はこちら 421
AmazonDetectiveServiceLinkedRolePolicy 421
このポリシーを使用すると 421
ポリシーの詳細 421
ポリシーのバージョン 422
JSON ポリシードキュメント 422
詳細はこちら 422
AmazonDevOpsGuruConsoleFullAccess 422
このポリシーを使用すると 422
ポリシーの詳細 423
ポリシーのバージョン 423
JSON ポリシードキュメント 423
詳細はこちら 425
AmazonDevOpsGuruFullAccess 426
このポリシーを使用すると 426
ポリシーの詳細 426
ポリシーのバージョン 426
JSON ポリシードキュメント 426
詳細はこちら 428
AmazonDevOpsGuruOrganizationsAccess 429
このポリシーを使用すると 429
ポリシーの詳細 429
ポリシーのバージョン 429
JSON ポリシードキュメント 429
詳細はこちら 430
AmazonDevOpsGuruReadOnlyAccess 431
このポリシーを使用すると 431
ポリシーの詳細 431
ポリシーのバージョン 431
JSON ポリシードキュメント 431
詳細はこちら 433

AmazonDevOpsGuruServiceRolePolicy 433
このポリシーを使用すると 434
ポリシーの詳細 434
ポリシーのバージョン 434
JSON ポリシードキュメント 434
詳細はこちら 438
AmazonDMSCloudWatchLogsRole 438
このポリシーを使用すると 438
ポリシーの詳細 439
ポリシーのバージョン 439
JSON ポリシードキュメント 439
詳細はこちら 440
AmazonDMSRedshiftS3Role 441
このポリシーを使用すると 441
ポリシーの詳細 441
ポリシーのバージョン 441
JSON ポリシードキュメント 441
詳細はこちら 442
AmazonDMSVPCManagementRole 442
このポリシーを使用すると 442
ポリシーの詳細 442
ポリシーのバージョン 443
JSON ポリシードキュメント 443
詳細はこちら 443
AmazonDocDB-ElasticServiceRolePolicy 444
このポリシーを使用すると 444
ポリシーの詳細 444
ポリシーのバージョン 444
JSON ポリシードキュメント 444
詳細はこちら 445
AmazonDocDBConsoleFullAccess 445
このポリシーを使用すると 445
ポリシーの詳細 445
ポリシーのバージョン 446
JSON ポリシードキュメント 446
詳細はこちら 450

AmazonDocDBElasticFullAccess 450
このポリシーを使用すると 451
ポリシーの詳細 451
ポリシーのバージョン 451
JSON ポリシードキュメント 451
詳細はこちら 454
AmazonDocDBElasticReadOnlyAccess 455
このポリシーを使用すると 455
ポリシーの詳細 455
ポリシーのバージョン 455
JSON ポリシードキュメント 455
詳細はこちら 456
AmazonDocDBFullAccess 456
このポリシーを使用すると 456
ポリシーの詳細 456
ポリシーのバージョン 457
JSON ポリシードキュメント 457
詳細はこちら 459
AmazonDocDBReadOnlyAccess 460
このポリシーを使用すると 460
ポリシーの詳細 460
ポリシーのバージョン 460
JSON ポリシードキュメント 460
詳細はこちら 462
AmazonDRSVPCManagement 462
このポリシーを使用すると 462
ポリシーの詳細 462
ポリシーのバージョン 463
JSON ポリシードキュメント 463
詳細はこちら 463
AmazonDynamoDBFullAccess 464
このポリシーを使用すると 464
ポリシーの詳細 464
ポリシーのバージョン 464
JSON ポリシードキュメント 464
詳細はこちら 467

AmazonDynamoDBFullAccess_v2 467
このポリシーを使用すると 467
ポリシーの詳細 467
ポリシーのバージョン 468
JSON ポリシードキュメント 468
詳細はこちら 471
AmazonDynamoDBFullAccesswithDataPipeline 471
このポリシーを使用すると 471
ポリシーの詳細 472
ポリシーのバージョン 472
JSON ポリシードキュメント 472
詳細はこちら 474
AmazonDynamoDBReadOnlyAccess 474
このポリシーを使用すると 474
ポリシーの詳細 474
ポリシーのバージョン 475
JSON ポリシードキュメント 475
詳細はこちら 477
AmazonEBSCSIDriverPolicy 477
このポリシーを使用すると 477
ポリシーの詳細 477
ポリシーのバージョン 477
JSON ポリシードキュメント 477
詳細はこちら 482
AmazonEC2ContainerRegistryFullAccess 482
このポリシーを使用すると 482
ポリシーの詳細 482
ポリシーのバージョン 483
JSON ポリシードキュメント 483
詳細はこちら 484
AmazonEC2ContainerRegistryPowerUser 484
このポリシーを使用すると 484
ポリシーの詳細 484
ポリシーのバージョン 484
JSON ポリシードキュメント 484
詳細はこちら 485

AmazonEC2ContainerRegistryPullOnly 485
このポリシーを使用すると 486
ポリシーの詳細 486
ポリシーのバージョン 486
JSON ポリシードキュメント 486
詳細はこちら 487
AmazonEC2ContainerRegistryReadOnly 487
このポリシーを使用すると 487
ポリシーの詳細 487
ポリシーのバージョン 487
JSON ポリシードキュメント 487
詳細はこちら 488
AmazonEC2ContainerServiceAutoscaleRole 488
このポリシーを使用すると 488
ポリシーの詳細 489
ポリシーのバージョン 489
JSON ポリシードキュメント 489
詳細はこちら 490
AmazonEC2ContainerServiceEventsRole 490
このポリシーを使用すると 490
ポリシーの詳細 490
ポリシーのバージョン 490
JSON ポリシードキュメント 491
詳細はこちら 492
AmazonEC2ContainerServiceforEC2Role 492
このポリシーを使用すると 492
ポリシーの詳細 492
ポリシーのバージョン 492
JSON ポリシードキュメント 492
詳細はこちら 494
AmazonEC2ContainerServiceRole 494
このポリシーを使用すると 494
ポリシーの詳細 494
ポリシーのバージョン 494
JSON ポリシードキュメント 495
詳細はこちら 495

AmazonEC2FullAccess 495
このポリシーを使用すると 495
ポリシーの詳細 496
ポリシーのバージョン 496
JSON ポリシードキュメント 496
詳細はこちら 497
AmazonEC2ImageReferencesAccessPolicy 497
このポリシーを使用すると 497
ポリシーの詳細 498
ポリシーのバージョン 498
JSON ポリシードキュメント 498
詳細はこちら 499
AmazonEC2ReadOnlyAccess 499
このポリシーを使用すると 499
ポリシーの詳細 499
ポリシーのバージョン 499
JSON ポリシードキュメント 500
詳細はこちら 500
AmazonEC2RoleforAWSCodeDeploy 501
このポリシーを使用すると 501
ポリシーの詳細 501
ポリシーのバージョン 501
JSON ポリシードキュメント 501
詳細はこちら 502
AmazonEC2RoleforAWSCodeDeployLimited 502
このポリシーを使用すると 502
ポリシーの詳細 502
ポリシーのバージョン 503
JSON ポリシードキュメント 503
詳細はこちら 503
AmazonEC2RoleforDataPipelineRole 504
このポリシーを使用すると 504
ポリシーの詳細 504
ポリシーのバージョン 504
JSON ポリシードキュメント 504
詳細はこちら 505

AmazonEC2RoleforSSM 505
このポリシーを使用すると 506
ポリシーの詳細 506
ポリシーのバージョン 506
JSON ポリシードキュメント 506
詳細はこちら 508
AmazonEC2RolePolicyForLaunchWizard 509
このポリシーを使用すると 509
ポリシーの詳細 509
ポリシーのバージョン 509
JSON ポリシードキュメント 509
詳細はこちら 513
AmazonEC2SpotFleetAutoscaleRole 513
このポリシーを使用すると 513
ポリシーの詳細 514
ポリシーのバージョン 514
JSON ポリシードキュメント 514
詳細はこちら 515
AmazonEC2SpotFleetTaggingRole 515
このポリシーを使用すると 515
ポリシーの詳細 515
ポリシーのバージョン 516
JSON ポリシードキュメント 516
詳細はこちら 517
AmazonECS_FullAccess 517
このポリシーを使用すると 517
ポリシーの詳細 518
ポリシーのバージョン 518
JSON ポリシードキュメント 518
詳細はこちら 524
AmazonECSComputeServiceRolePolicy 524
このポリシーを使用すると 524
ポリシーの詳細 524
ポリシーのバージョン 525
JSON ポリシードキュメント 525
詳細はこちら 526

AmazonECSInfrastructureRoleforExpressGatewayServices 526
このポリシーを使用すると 527
ポリシーの詳細 527
ポリシーのバージョン 527
JSON ポリシードキュメント 527
詳細はこちら 533
AmazonECSInfrastructureRolePolicyForLoadBalancers 534
このポリシーを使用すると 534
ポリシーの詳細 534
ポリシーのバージョン 534
JSON ポリシードキュメント 534
詳細はこちら 536
AmazonECSInfrastructureRolePolicyForManagedInstances 536
このポリシーを使用すると 536
ポリシーの詳細 536
ポリシーのバージョン 536
JSON ポリシードキュメント 537
詳細はこちら 541
AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity 541
このポリシーを使用すると 541
ポリシーの詳細 541
ポリシーのバージョン 541
JSON ポリシードキュメント 542
詳細はこちら 544
AmazonECSInfrastructureRolePolicyForVolumes 544
このポリシーを使用すると 544
ポリシーの詳細 545
ポリシーのバージョン 545
JSON ポリシードキュメント 545
詳細はこちら 547
AmazonECSInfrastructureRolePolicyForVpcLattice 547
このポリシーを使用すると 548
ポリシーの詳細 548
ポリシーのバージョン 548
JSON ポリシードキュメント 548
詳細はこちら 549

AmazonECSInstanceRolePolicyForManagedInstances 550
このポリシーを使用すると 550
ポリシーの詳細 550
ポリシーのバージョン 550
JSON ポリシードキュメント 550
詳細はこちら 551
AmazonECSServiceRolePolicy 552
このポリシーを使用すると 552
ポリシーの詳細 552
ポリシーのバージョン 552
JSON ポリシードキュメント 552
詳細はこちら 558
AmazonECSTaskExecutionRolePolicy 558
このポリシーを使用すると 558
ポリシーの詳細 558
ポリシーのバージョン 558
JSON ポリシードキュメント 558
詳細はこちら 559
AmazonEFSCSIDriverPolicy 559
このポリシーを使用すると 559
ポリシーの詳細 559
ポリシーのバージョン 560
JSON ポリシードキュメント 560
詳細はこちら 561
AmazonEKS_CNI_Policy 562
このポリシーを使用すると 562
ポリシーの詳細 562
ポリシーのバージョン 562
JSON ポリシードキュメント 562
詳細はこちら 563
AmazonEKSBlockStoragePolicy 563
このポリシーを使用すると 564
ポリシーの詳細 564
ポリシーのバージョン 564
JSON ポリシードキュメント 564
詳細はこちら 566

AmazonEKSClusterPolicy 567
このポリシーを使用すると 567
ポリシーの詳細 567
ポリシーのバージョン 567
JSON ポリシードキュメント 567
詳細はこちら 570
AmazonEKSComputePolicy 570
このポリシーを使用すると 570
ポリシーの詳細 570
ポリシーのバージョン 570
JSON ポリシードキュメント 570
詳細はこちら 573
AmazonEKSConnectorServiceRolePolicy 573
このポリシーを使用すると 573
ポリシーの詳細 573
ポリシーのバージョン 574
JSON ポリシードキュメント 574
詳細はこちら 576
AmazonEKSDashboardConsoleReadOnly 576
このポリシーを使用すると 576
ポリシーの詳細 576
ポリシーのバージョン 577
JSON ポリシードキュメント 577
詳細はこちら 578
AmazonEKSDashboardServiceRolePolicy 578
このポリシーを使用すると 578
ポリシーの詳細 578
ポリシーのバージョン 579
JSON ポリシードキュメント 579
詳細はこちら 579
AmazonEKSFargatePodExecutionRolePolicy 579
このポリシーを使用すると 580
ポリシーの詳細 580
ポリシーのバージョン 580
JSON ポリシードキュメント 580
詳細はこちら 581

AmazonEKSForFargateServiceRolePolicy 581
このポリシーを使用すると 581
ポリシーの詳細 581
ポリシーのバージョン 581
JSON ポリシードキュメント 582
詳細はこちら 582
AmazonEKSLoadBalancingPolicy 582
このポリシーを使用すると 582
ポリシーの詳細 583
ポリシーのバージョン 583
JSON ポリシードキュメント 583
詳細はこちら 589
AmazonEKSLocalOutpostClusterPolicy 589
このポリシーを使用すると 589
ポリシーの詳細 590
ポリシーのバージョン 590
JSON ポリシードキュメント 590
詳細はこちら 592
AmazonEKSLocalOutpostServiceRolePolicy 592
このポリシーを使用すると 592
ポリシーの詳細 592
ポリシーのバージョン 593
JSON ポリシードキュメント 593
詳細はこちら 598
AmazonEKSMCPReadOnlyAccess 599
このポリシーを使用すると 599
ポリシーの詳細 599
ポリシーのバージョン 599
JSON ポリシードキュメント 599
詳細はこちら 601
AmazonEKSNetworkingPolicy 601
このポリシーを使用すると 601
ポリシーの詳細 601
ポリシーのバージョン 602
JSON ポリシードキュメント 602
詳細はこちら 603

AmazonEKSServicePolicy 604
このポリシーを使用すると 604
ポリシーの詳細 604
ポリシーのバージョン 604
JSON ポリシードキュメント 604
詳細はこちら 606
AmazonEKSServiceRolePolicy 606
このポリシーを使用すると 607
ポリシーの詳細 607
ポリシーのバージョン 607
JSON ポリシードキュメント 607
詳細はこちら 615
AmazonEKSVPCResourceController 615
このポリシーを使用すると 615
ポリシーの詳細 615
ポリシーのバージョン 615
JSON ポリシードキュメント 616
詳細はこちら 616
AmazonEKSWorkerNodeMinimalPolicy 617
このポリシーを使用すると 617
ポリシーの詳細 617
ポリシーのバージョン 617
JSON ポリシードキュメント 617
詳細はこちら 618
AmazonEKSWorkerNodePolicy 618
このポリシーを使用すると 618
ポリシーの詳細 618
ポリシーのバージョン 618
JSON ポリシードキュメント 619
詳細はこちら 619
AmazonElastiCacheFullAccess 619
このポリシーを使用すると 620
ポリシーの詳細 620
ポリシーのバージョン 620
JSON ポリシードキュメント 620
詳細はこちら 623

AmazonElastiCacheReadOnlyAccess 624
このポリシーを使用すると 624
ポリシーの詳細 624
ポリシーのバージョン 624
JSON ポリシードキュメント 624
詳細はこちら 625
AmazonElasticContainerRegistryPublicFullAccess 625
このポリシーを使用すると 625
ポリシーの詳細 625
ポリシーのバージョン 625
JSON ポリシードキュメント 626
詳細はこちら 626
AmazonElasticContainerRegistryPublicPowerUser 626
このポリシーを使用すると 626
ポリシーの詳細 626
ポリシーのバージョン 627
JSON ポリシードキュメント 627
詳細はこちら 628
AmazonElasticContainerRegistryPublicReadOnly 628
このポリシーを使用すると 628
ポリシーの詳細 628
ポリシーのバージョン 628
JSON ポリシードキュメント 628
詳細はこちら 629
AmazonElasticFileSystemClientFullAccess 629
このポリシーを使用すると 629
ポリシーの詳細 630
ポリシーのバージョン 630
JSON ポリシードキュメント 630
詳細はこちら 630
AmazonElasticFileSystemClientReadOnlyAccess 631
このポリシーを使用すると 631
ポリシーの詳細 631
ポリシーのバージョン 631
JSON ポリシードキュメント 631
詳細はこちら 632

AmazonElasticFileSystemClientReadWriteAccess 632
このポリシーを使用すると 632
ポリシーの詳細 632
ポリシーのバージョン 632
JSON ポリシードキュメント 633
詳細はこちら 633
AmazonElasticFileSystemFullAccess 633
このポリシーを使用すると 633
ポリシーの詳細 633
ポリシーのバージョン 634
JSON ポリシードキュメント 634
詳細はこちら 636
AmazonElasticFileSystemReadOnlyAccess 636
このポリシーを使用すると 636
ポリシーの詳細 636
ポリシーのバージョン 637
JSON ポリシードキュメント 637
詳細はこちら 638
AmazonElasticFileSystemServiceRolePolicy 638
このポリシーを使用すると 638
ポリシーの詳細 638
ポリシーのバージョン 638
JSON ポリシードキュメント 639
詳細はこちら 641
AmazonElasticFileSystemsUtils 641
このポリシーを使用すると 641
ポリシーの詳細 641
ポリシーのバージョン 641
JSON ポリシードキュメント 641
詳細はこちら 643
AmazonElasticMapReduceEditorsRole 643
このポリシーを使用すると 644
ポリシーの詳細 644
ポリシーのバージョン 644
JSON ポリシードキュメント 644
詳細はこちら 645

AmazonElasticMapReduceforAutoScalingRole 645
このポリシーを使用すると 646
ポリシーの詳細 646
ポリシーのバージョン 646
JSON ポリシードキュメント 646
詳細はこちら 647
AmazonElasticMapReduceforEC2Role 647
このポリシーを使用すると 647
ポリシーの詳細 647
ポリシーのバージョン 647
JSON ポリシードキュメント 648
詳細はこちら 649
AmazonElasticMapReduceFullAccess 649
このポリシーを使用すると 649
ポリシーの詳細 650
ポリシーのバージョン 650
JSON ポリシードキュメント 650
詳細はこちら 652
AmazonElasticMapReducePlacementGroupPolicy 652
このポリシーを使用すると 652
ポリシーの詳細 652
ポリシーのバージョン 652
JSON ポリシードキュメント 652
詳細はこちら 653
AmazonElasticMapReduceReadOnlyAccess 653
このポリシーを使用すると 653
ポリシーの詳細 654
ポリシーのバージョン 654
JSON ポリシードキュメント 654
詳細はこちら 655
AmazonElasticMapReduceRole 655
このポリシーを使用すると 655
ポリシーの詳細 655
ポリシーのバージョン 655
JSON ポリシードキュメント 655
詳細はこちら 658

AmazonElasticsearchServiceRolePolicy 658
このポリシーを使用すると 658
ポリシーの詳細 658
ポリシーのバージョン 658
JSON ポリシードキュメント 659
詳細はこちら 661
AmazonElasticTranscoder_FullAccess 661
このポリシーを使用すると 662
ポリシーの詳細 662
ポリシーのバージョン 662
JSON ポリシードキュメント 662
詳細はこちら 663
AmazonElasticTranscoder_JobsSubmitter 663
このポリシーを使用すると 663
ポリシーの詳細 663
ポリシーのバージョン 664
JSON ポリシードキュメント 664
詳細はこちら 664
AmazonElasticTranscoder_ReadOnlyAccess 665
このポリシーを使用すると 665
ポリシーの詳細 665
ポリシーのバージョン 665
JSON ポリシードキュメント 665
詳細はこちら 666
AmazonElasticTranscoderRole 666
このポリシーを使用すると 666
ポリシーの詳細 666
ポリシーのバージョン 666
JSON ポリシードキュメント 667
詳細はこちら 667
AmazonEMRCleanupPolicy 668
このポリシーを使用すると 668
ポリシーの詳細 668
ポリシーのバージョン 668
JSON ポリシードキュメント 668
詳細はこちら 669

AmazonEMRContainersServiceRolePolicy 669
このポリシーを使用すると 669
ポリシーの詳細 669
ポリシーのバージョン 670
JSON ポリシードキュメント 670
詳細はこちら 671
AmazonEMRFullAccessPolicy_v2 671
このポリシーを使用すると 671
ポリシーの詳細 671
ポリシーのバージョン 672
JSON ポリシードキュメント 672
詳細はこちら 675
AmazonEMRReadOnlyAccessPolicy_v2 675
このポリシーを使用すると 676
ポリシーの詳細 676
ポリシーのバージョン 676
JSON ポリシードキュメント 676
詳細はこちら 677
AmazonEMRServerlessServiceRolePolicy 677
このポリシーを使用すると 678
ポリシーの詳細 678
ポリシーのバージョン 678
JSON ポリシードキュメント 678
詳細はこちら 679
AmazonEMRServicePolicy_v2 679
このポリシーを使用すると 679
ポリシーの詳細 680
ポリシーのバージョン 680
JSON ポリシードキュメント 680
詳細はこちら 689
AmazonESCognitoAccess 689
このポリシーを使用すると 689
ポリシーの詳細 689
ポリシーのバージョン 689
JSON ポリシードキュメント 690
詳細はこちら 690

AmazonESFullAccess ... 691
このポリシーを使用すると ... 691
ポリシーの詳細 ... 691
ポリシーのバージョン ... 691
JSON ポリシードキュメント ... 691
詳細はこちら ... 692
AmazonESReadOnlyAccess ... 692
このポリシーを使用すると ... 692
ポリシーの詳細 ... 692
ポリシーのバージョン ... 692
JSON ポリシードキュメント ... 693
詳細はこちら ... 693
AmazonEventBridgeApiDestinationsServiceRolePolicy ... 693
このポリシーを使用すると ... 693
ポリシーの詳細 ... 694
ポリシーのバージョン ... 694
JSON ポリシードキュメント ... 694
詳細はこちら ... 695
AmazonEventBridgeFullAccess ... 695
このポリシーを使用すると ... 695
ポリシーの詳細 ... 695
ポリシーのバージョン ... 696
JSON ポリシードキュメント ... 696
詳細はこちら ... 698
AmazonEventBridgePipesFullAccess ... 698
このポリシーを使用すると ... 698
ポリシーの詳細 ... 698
ポリシーのバージョン ... 699
JSON ポリシードキュメント ... 699
詳細はこちら ... 699
AmazonEventBridgePipesOperatorAccess ... 700
このポリシーを使用すると ... 700
ポリシーの詳細 ... 700
ポリシーのバージョン ... 700
JSON ポリシードキュメント ... 700
詳細はこちら ... 701

AmazonEventBridgePipesReadOnlyAccess 701
このポリシーを使用すると 701
ポリシーの詳細 701
ポリシーのバージョン 701
JSON ポリシードキュメント 702
詳細はこちら 702
AmazonEventBridgeReadOnlyAccess 702
このポリシーを使用すると 702
ポリシーの詳細 702
ポリシーのバージョン 703
JSON ポリシードキュメント 703
詳細はこちら 704
AmazonEventBridgeSchedulerFullAccess 704
このポリシーを使用すると 705
ポリシーの詳細 705
ポリシーのバージョン 705
JSON ポリシードキュメント 705
詳細はこちら 706
AmazonEventBridgeSchedulerReadOnlyAccess 706
このポリシーを使用すると 706
ポリシーの詳細 706
ポリシーのバージョン 706
JSON ポリシードキュメント 707
詳細はこちら 707
AmazonEventBridgeSchemasFullAccess 707
このポリシーを使用すると 707
ポリシーの詳細 708
ポリシーのバージョン 708
JSON ポリシードキュメント 708
詳細はこちら 709
AmazonEventBridgeSchemasReadOnlyAccess 709
このポリシーを使用すると 709
ポリシーの詳細 709
ポリシーのバージョン 710
JSON ポリシードキュメント 710
詳細はこちら 710

AmazonEventBridgeSchemasServiceRolePolicy 711
このポリシーを使用すると 711
ポリシーの詳細 711
ポリシーのバージョン 711
JSON ポリシードキュメント 711
詳細はこちら 712
AmazonEVSServiceRolePolicy 712
このポリシーを使用すると 712
ポリシーの詳細 712
ポリシーのバージョン 713
JSON ポリシードキュメント 713
詳細はこちら 717
AmazonFISServiceRolePolicy 717
このポリシーを使用すると 717
ポリシーの詳細 717
ポリシーのバージョン 717
JSON ポリシードキュメント 717
詳細はこちら 719
AmazonForecastFullAccess 719
このポリシーを使用すると 719
ポリシーの詳細 719
ポリシーのバージョン 720
JSON ポリシードキュメント 720
詳細はこちら 720
AmazonFraudDetectorFullAccessPolicy 721
このポリシーを使用すると 721
ポリシーの詳細 721
ポリシーのバージョン 721
JSON ポリシードキュメント 721
詳細はこちら 723
AmazonFreeRTOSFullAccess 723
このポリシーを使用すると 723
ポリシーの詳細 723
ポリシーのバージョン 723
JSON ポリシードキュメント 723
詳細はこちら 724

AmazonFreeRTOSOTAUpdate 724
このポリシーを使用すると 724
ポリシーの詳細 724
ポリシーのバージョン 724
JSON ポリシードキュメント 725
詳細はこちら 726
AmazonFSxConsoleFullAccess 726
このポリシーを使用すると 726
ポリシーの詳細 727
ポリシーのバージョン 727
JSON ポリシードキュメント 727
詳細はこちら 730
AmazonFSxConsoleReadOnlyAccess 731
このポリシーを使用すると 731
ポリシーの詳細 731
ポリシーのバージョン 731
JSON ポリシードキュメント 731
詳細はこちら 732
AmazonFSxFullAccess 732
このポリシーを使用すると 732
ポリシーの詳細 732
ポリシーのバージョン 733
JSON ポリシードキュメント 733
詳細はこちら 737
AmazonFSxReadOnlyAccess 737
このポリシーを使用すると 737
ポリシーの詳細 737
ポリシーのバージョン 738
JSON ポリシードキュメント 738
詳細はこちら 738
AmazonFSxServiceRolePolicy 738
このポリシーを使用すると 739
ポリシーの詳細 739
ポリシーのバージョン 739
JSON ポリシードキュメント 739
詳細はこちら 742

AmazonGlacierFullAccess 742
このポリシーを使用すると 742
ポリシーの詳細 742
ポリシーのバージョン 742
JSON ポリシードキュメント 743
詳細はこちら 743
AmazonGlacierReadOnlyAccess 743
このポリシーを使用すると 743
ポリシーの詳細 743
ポリシーのバージョン 744
JSON ポリシードキュメント 744
詳細はこちら 744
AmazonGrafanaAthenaAccess 745
このポリシーを使用すると 745
ポリシーの詳細 745
ポリシーのバージョン 745
JSON ポリシードキュメント 745
詳細はこちら 747
AmazonGrafanaCloudWatchAccess 747
このポリシーを使用すると 747
ポリシーの詳細 748
ポリシーのバージョン 748
JSON ポリシードキュメント 748
詳細はこちら 749
AmazonGrafanaRedshiftAccess 750
このポリシーを使用すると 750
ポリシーの詳細 750
ポリシーのバージョン 750
JSON ポリシードキュメント 750
詳細はこちら 751
AmazonGrafanaServiceLinkedRolePolicy 752
このポリシーを使用すると 752
ポリシーの詳細 752
ポリシーのバージョン 752
JSON ポリシードキュメント 752
詳細はこちら 754

AmazonGuardDutyFullAccess 754
このポリシーを使用すると 754
ポリシーの詳細 754
ポリシーのバージョン 754
JSON ポリシードキュメント 754
詳細はこちら 756
AmazonGuardDutyFullAccess_v2 756
このポリシーを使用すると 756
ポリシーの詳細 756
ポリシーのバージョン 757
JSON ポリシードキュメント 757
詳細はこちら 759
AmazonGuardDutyMalwareProtectionServiceRolePolicy 759
このポリシーを使用すると 759
ポリシーの詳細 759
ポリシーのバージョン 760
JSON ポリシードキュメント 760
詳細はこちら 764
AmazonGuardDutyReadOnlyAccess 764
このポリシーを使用すると 765
ポリシーの詳細 765
ポリシーのバージョン 765
JSON ポリシードキュメント 765
詳細はこちら 766
AmazonGuardDutyServiceRolePolicy 766
このポリシーを使用すると 766
ポリシーの詳細 766
ポリシーのバージョン 767
JSON ポリシードキュメント 767
詳細はこちら 773
AmazonHealthLakeFullAccess 773
このポリシーを使用すると 773
ポリシーの詳細 773
ポリシーのバージョン 773
JSON ポリシードキュメント 774
詳細はこちら 774

AmazonHealthLakeReadOnlyAccess 774
このポリシーを使用すると 775
ポリシーの詳細 775
ポリシーのバージョン 775
JSON ポリシードキュメント 775
詳細はこちら 776
AmazonHoneycodeFullAccess 776
このポリシーを使用すると 776
ポリシーの詳細 776
ポリシーのバージョン 776
JSON ポリシードキュメント 777
詳細はこちら 777
AmazonHoneycodeReadOnlyAccess 777
このポリシーを使用すると 777
ポリシーの詳細 777
ポリシーのバージョン 778
JSON ポリシードキュメント 778
詳細はこちら 778
AmazonHoneycodeServiceRolePolicy 778
このポリシーを使用すると 779
ポリシーの詳細 779
ポリシーのバージョン 779
JSON ポリシードキュメント 779
詳細はこちら 780
AmazonHoneycodeTeamAssociationFullAccess 780
このポリシーを使用すると 780
ポリシーの詳細 780
ポリシーのバージョン 780
JSON ポリシードキュメント 780
詳細はこちら 781
AmazonHoneycodeTeamAssociationReadOnlyAccess 781
このポリシーを使用すると 781
ポリシーの詳細 781
ポリシーのバージョン 782
JSON ポリシードキュメント 782
詳細はこちら 782

AmazonHoneycodeWorkbookFullAccess 782
このポリシーを使用すると 783
ポリシーの詳細 783
ポリシーのバージョン 783
JSON ポリシードキュメント 783
詳細はこちら 784
AmazonHoneycodeWorkbookReadOnlyAccess 784
このポリシーを使用すると 784
ポリシーの詳細 784
ポリシーのバージョン 784
JSON ポリシードキュメント 785
詳細はこちら 785
AmazonInspector2AgentlessServiceRolePolicy 785
このポリシーを使用すると 786
ポリシーの詳細 786
ポリシーのバージョン 786
JSON ポリシードキュメント 786
詳細はこちら 790
AmazonInspector2FullAccess 790
このポリシーを使用すると 790
ポリシーの詳細 790
ポリシーのバージョン 790
JSON ポリシードキュメント 791
詳細はこちら 792
AmazonInspector2FullAccess_v2 792
このポリシーを使用すると 792
ポリシーの詳細 792
ポリシーのバージョン 792
JSON ポリシードキュメント 793
詳細はこちら 795
AmazonInspector2ManagedCisPolicy 795
このポリシーを使用すると 796
ポリシーの詳細 796
ポリシーのバージョン 796
JSON ポリシードキュメント 796
詳細はこちら 797

AmazonInspector2ReadOnlyAccess 797
このポリシーを使用すると 797
ポリシーの詳細 797
ポリシーのバージョン 797
JSON ポリシードキュメント 797
詳細はこちら 799
AmazonInspector2ServiceRolePolicy 799
このポリシーを使用すると 799
ポリシーの詳細 799
ポリシーのバージョン 800
JSON ポリシードキュメント 800
詳細はこちら 808
AmazonInspectorFullAccess 808
このポリシーを使用すると 808
ポリシーの詳細 808
ポリシーのバージョン 808
JSON ポリシードキュメント 808
詳細はこちら 810
AmazonInspectorReadOnlyAccess 810
このポリシーを使用すると 810
ポリシーの詳細 810
ポリシーのバージョン 810
JSON ポリシードキュメント 810
詳細はこちら 811
AmazonInspectorServiceRolePolicy 811
このポリシーを使用すると 811
ポリシーの詳細 812
ポリシーのバージョン 812
JSON ポリシードキュメント 812
詳細はこちら 813
AmazonKendraFullAccess 813
このポリシーを使用すると 814
ポリシーの詳細 814
ポリシーのバージョン 814
JSON ポリシードキュメント 814
詳細はこちら 816

AmazonKendraReadOnlyAccess 816
このポリシーを使用すると 816
ポリシーの詳細 816
ポリシーのバージョン 817
JSON ポリシードキュメント 817
詳細はこちら 817
AmazonKeyspacesFullAccess 817
このポリシーを使用すると 818
ポリシーの詳細 818
ポリシーのバージョン 818
JSON ポリシードキュメント 818
詳細はこちら 820
AmazonKeyspacesReadOnlyAccess 820
このポリシーを使用すると 821
ポリシーの詳細 821
ポリシーのバージョン 821
JSON ポリシードキュメント 821
詳細はこちら 822
AmazonKeyspacesReadOnlyAccess_v2 822
このポリシーを使用すると 822
ポリシーの詳細 822
ポリシーのバージョン 823
JSON ポリシードキュメント 823
詳細はこちら 824
AmazonKinesisAnalyticsFullAccess 824
このポリシーを使用すると 824
ポリシーの詳細 824
ポリシーのバージョン 824
JSON ポリシードキュメント 825
詳細はこちら 826
AmazonKinesisAnalyticsReadOnly 826
このポリシーを使用すると 826
ポリシーの詳細 827
ポリシーのバージョン 827
JSON ポリシードキュメント 827
詳細はこちら 828

AmazonKinesisFirehoseFullAccess 828
このポリシーを使用すると 829
ポリシーの詳細 829
ポリシーのバージョン 829
JSON ポリシードキュメント 829
詳細はこちら 829
AmazonKinesisFirehoseReadOnlyAccess 830
このポリシーを使用すると 830
ポリシーの詳細 830
ポリシーのバージョン 830
JSON ポリシードキュメント 830
詳細はこちら 831
AmazonKinesisFullAccess 831
このポリシーを使用すると 831
ポリシーの詳細 831
ポリシーのバージョン 831
JSON ポリシードキュメント 832
詳細はこちら 832
AmazonKinesisReadOnlyAccess 832
このポリシーを使用すると 832
ポリシーの詳細 832
ポリシーのバージョン 833
JSON ポリシードキュメント 833
詳細はこちら 833
AmazonKinesisVideoStreamsFullAccess 834
このポリシーを使用すると 834
ポリシーの詳細 834
ポリシーのバージョン 834
JSON ポリシードキュメント 834
詳細はこちら 835
AmazonKinesisVideoStreamsReadOnlyAccess 835
このポリシーを使用すると 835
ポリシーの詳細 835
ポリシーのバージョン 835
JSON ポリシードキュメント 835
詳細はこちら 836

AmazonLaunchWizard_Fullaccess 836
このポリシーを使用すると 836
ポリシーの詳細 836
ポリシーのバージョン 837
JSON ポリシードキュメント 837
詳細はこちら 851
AmazonLaunchWizardFullAccessV2 851
このポリシーを使用すると 851
ポリシーの詳細 851
ポリシーのバージョン 852
JSON ポリシードキュメント 852
詳細はこちら 868
AmazonLexChannelsAccess 868
このポリシーを使用すると 869
ポリシーの詳細 869
ポリシーのバージョン 869
JSON ポリシードキュメント 869
詳細はこちら 869
AmazonLexFullAccess 870
このポリシーを使用すると 870
ポリシーの詳細 870
ポリシーのバージョン 870
JSON ポリシードキュメント 870
詳細はこちら 876
AmazonLexReadOnly 876
このポリシーを使用すると 876
ポリシーの詳細 876
ポリシーのバージョン 876
JSON ポリシードキュメント 877
詳細はこちら 878
AmazonLexReplicationPolicy 878
このポリシーを使用すると 879
ポリシーの詳細 879
ポリシーのバージョン 879
JSON ポリシードキュメント 879
詳細はこちら 881

AmazonLexRunBotsOnly 882
このポリシーを使用すると 882
ポリシーの詳細 882
ポリシーのバージョン 882
JSON ポリシードキュメント 882
詳細はこちら 883
AmazonLexV2BotPolicy 883
このポリシーを使用すると 883
ポリシーの詳細 883
ポリシーのバージョン 883
JSON ポリシードキュメント 884
詳細はこちら 884
AmazonLookoutEquipmentFullAccess 884
このポリシーを使用すると 884
ポリシーの詳細 884
ポリシーのバージョン 885
JSON ポリシードキュメント 885
詳細はこちら 886
AmazonLookoutEquipmentReadOnlyAccess 886
このポリシーを使用すると 886
ポリシーの詳細 887
ポリシーのバージョン 887
JSON ポリシードキュメント 887
詳細はこちら 887
AmazonLookoutMetricsFullAccess 888
このポリシーを使用すると 888
ポリシーの詳細 888
ポリシーのバージョン 888
JSON ポリシードキュメント 888
詳細はこちら 889
AmazonLookoutMetricsReadOnlyAccess 889
このポリシーを使用すると 889
ポリシーの詳細 889
ポリシーのバージョン 890
JSON ポリシードキュメント 890
詳細はこちら 890

AmazonLookoutVisionConsoleFullAccess 891
このポリシーを使用すると 891
ポリシーの詳細 891
ポリシーのバージョン 891
JSON ポリシードキュメント 891
詳細はこちら 894
AmazonLookoutVisionConsoleReadOnlyAccess 894
このポリシーを使用すると 894
ポリシーの詳細 894
ポリシーのバージョン 894
JSON ポリシードキュメント 894
詳細はこちら 896
AmazonLookoutVisionFullAccess 896
このポリシーを使用すると 896
ポリシーの詳細 896
ポリシーのバージョン 896
JSON ポリシードキュメント 897
詳細はこちら 897
AmazonLookoutVisionReadOnlyAccess 897
このポリシーを使用すると 897
ポリシーの詳細 897
ポリシーのバージョン 898
JSON ポリシードキュメント 898
詳細はこちら 898
AmazonMachineLearningBatchPredictionsAccess 899
このポリシーを使用すると 899
ポリシーの詳細 899
ポリシーのバージョン 899
JSON ポリシードキュメント 899
詳細はこちら 900
AmazonMachineLearningCreateOnlyAccess 900
このポリシーを使用すると 900
ポリシーの詳細 900
ポリシーのバージョン 901
JSON ポリシードキュメント 901
詳細はこちら 901

AmazonMachineLearningFullAccess 901
このポリシーを使用すると 902
ポリシーの詳細 902
ポリシーのバージョン 902
JSON ポリシードキュメント 902
詳細はこちら 902
AmazonMachineLearningManageRealTimeEndpointOnlyAccess 903
このポリシーを使用すると 903
ポリシーの詳細 903
ポリシーのバージョン 903
JSON ポリシードキュメント 903
詳細はこちら 904
AmazonMachineLearningReadOnlyAccess 904
このポリシーを使用すると 904
ポリシーの詳細 904
ポリシーのバージョン 904
JSON ポリシードキュメント 905
詳細はこちら 905
AmazonMachineLearningRealTimePredictionOnlyAccess 905
このポリシーを使用すると 905
ポリシーの詳細 906
ポリシーのバージョン 906
JSON ポリシードキュメント 906
詳細はこちら 906
AmazonMachineLearningRoleforRedshiftDataSourceV3 907
このポリシーを使用すると 907
ポリシーの詳細 907
ポリシーのバージョン 907
JSON ポリシードキュメント 907
詳細はこちら 908
AmazonMacieFullAccess 908
このポリシーを使用すると 908
ポリシーの詳細 909
ポリシーのバージョン 909
JSON ポリシードキュメント 909
詳細はこちら 910

AmazonMacieHandshakeRole 910
このポリシーを使用すると 910
ポリシーの詳細 910
ポリシーのバージョン 910
JSON ポリシードキュメント 911
詳細はこちら 911
AmazonMacieReadOnlyAccess 911
このポリシーを使用すると 911
ポリシーの詳細 911
ポリシーのバージョン 912
JSON ポリシードキュメント 912
詳細はこちら 912
AmazonMacieServiceRole 913
このポリシーを使用すると 913
ポリシーの詳細 913
ポリシーのバージョン 913
JSON ポリシードキュメント 913
詳細はこちら 914
AmazonMacieServiceRolePolicy 914
このポリシーを使用すると 914
ポリシーの詳細 914
ポリシーのバージョン 914
JSON ポリシードキュメント 915
詳細はこちら 916
AmazonManagedBlockchainConsoleFullAccess 916
このポリシーを使用すると 916
ポリシーの詳細 916
ポリシーのバージョン 917
JSON ポリシードキュメント 917
詳細はこちら 917
AmazonManagedBlockchainFullAccess 917
このポリシーを使用すると 918
ポリシーの詳細 918
ポリシーのバージョン 918
JSON ポリシードキュメント 918
詳細はこちら 919

AmazonManagedBlockchainReadOnlyAccess 919
このポリシーを使用すると 919
ポリシーの詳細 919
ポリシーのバージョン 919
JSON ポリシードキュメント 919
詳細はこちら 920
AmazonManagedBlockchainServiceRolePolicy 920
このポリシーを使用すると 920
ポリシーの詳細 920
ポリシーのバージョン 921
JSON ポリシードキュメント 921
詳細はこちら 921
AmazonMCSFullAccess 922
このポリシーを使用すると 922
ポリシーの詳細 922
ポリシーのバージョン 922
JSON ポリシードキュメント 922
詳細はこちら 923
AmazonMCSReadOnlyAccess 924
このポリシーを使用すると 924
ポリシーの詳細 924
ポリシーのバージョン 924
JSON ポリシードキュメント 924
詳細はこちら 925
AmazonMechanicalTurkFullAccess 925
このポリシーを使用すると 925
ポリシーの詳細 925
ポリシーのバージョン 926
JSON ポリシードキュメント 926
詳細はこちら 926
AmazonMechanicalTurkReadOnly 926
このポリシーを使用すると 927
ポリシーの詳細 927
ポリシーのバージョン 927
JSON ポリシードキュメント 927
詳細はこちら 928

AmazonMemoryDBFullAccess 928
このポリシーを使用すると 928
ポリシーの詳細 928
ポリシーのバージョン 928
JSON ポリシードキュメント 928
詳細はこちら 929
AmazonMemoryDBReadOnlyAccess 929
このポリシーを使用すると 929
ポリシーの詳細 929
ポリシーのバージョン 930
JSON ポリシードキュメント 930
詳細はこちら 930
AmazonMobileAnalyticsFinancialReportAccess 930
このポリシーを使用すると 931
ポリシーの詳細 931
ポリシーのバージョン 931
JSON ポリシードキュメント 931
詳細はこちら 932
AmazonMobileAnalyticsFullAccess 932
このポリシーを使用すると 932
ポリシーの詳細 932
ポリシーのバージョン 932
JSON ポリシードキュメント 932
詳細はこちら 933
AmazonMobileAnalyticsNon-financialReportAccess 933
このポリシーを使用すると 933
ポリシーの詳細 933
ポリシーのバージョン 934
JSON ポリシードキュメント 934
詳細はこちら 934
AmazonMobileAnalyticsWriteOnlyAccess 934
このポリシーを使用すると 934
ポリシーの詳細 935
ポリシーのバージョン 935
JSON ポリシードキュメント 935
詳細はこちら 935

AmazonMonitronFullAccess 936
このポリシーを使用すると 936
ポリシーの詳細 936
ポリシーのバージョン 936
JSON ポリシードキュメント 936
詳細はこちら 938
AmazonMQApiFullAccess 938
このポリシーを使用すると 938
ポリシーの詳細 938
ポリシーのバージョン 939
JSON ポリシードキュメント 939
詳細はこちら 940
AmazonMQApiReadOnlyAccess 940
このポリシーを使用すると 940
ポリシーの詳細 940
ポリシーのバージョン 941
JSON ポリシードキュメント 941
詳細はこちら 941
AmazonMQFullAccess 941
このポリシーを使用すると 942
ポリシーの詳細 942
ポリシーのバージョン 942
JSON ポリシードキュメント 942
詳細はこちら 943
AmazonMQReadOnlyAccess 943
このポリシーを使用すると 944
ポリシーの詳細 944
ポリシーのバージョン 944
JSON ポリシードキュメント 944
詳細はこちら 945
AmazonMQServiceRolePolicy 945
このポリシーを使用すると 945
ポリシーの詳細 945
ポリシーのバージョン 945
JSON ポリシードキュメント 946
詳細はこちら 947

AmazonMSKConnectReadOnlyAccess 948
このポリシーを使用すると 948
ポリシーの詳細 948
ポリシーのバージョン 948
JSON ポリシードキュメント 948
詳細はこちら 949
AmazonMSKFullAccess 949
このポリシーを使用すると 950
ポリシーの詳細 950
ポリシーのバージョン 950
JSON ポリシードキュメント 950
詳細はこちら 953
AmazonMSKReadOnlyAccess 953
このポリシーを使用すると 953
ポリシーの詳細 953
ポリシーのバージョン 954
JSON ポリシードキュメント 954
詳細はこちら 954
AmazonMWAAServerlessServiceRolePolicy 955
このポリシーを使用すると 955
ポリシーの詳細 955
ポリシーのバージョン 955
JSON ポリシードキュメント 955
詳細はこちら 956
AmazonMWAAServiceRolePolicy 956
このポリシーを使用すると 956
ポリシーの詳細 956
ポリシーのバージョン 957
JSON ポリシードキュメント 957
詳細はこちら 959
AmazonNimbleStudio-LaunchProfileWorker 959
このポリシーを使用すると 959
ポリシーの詳細 959
ポリシーのバージョン 960
JSON ポリシードキュメント 960
詳細はこちら 960

AmazonNimbleStudio-StudioAdmin 961
このポリシーを使用すると 961
ポリシーの詳細 961
ポリシーのバージョン 961
JSON ポリシードキュメント 961
詳細はこちら 963
AmazonNimbleStudio-StudioUser 963
このポリシーを使用すると 964
ポリシーの詳細 964
ポリシーのバージョン 964
JSON ポリシードキュメント 964
詳細はこちら 966
AmazonODBServiceRolePolicy 966
このポリシーを使用すると 967
ポリシーの詳細 967
ポリシーのバージョン 967
JSON ポリシードキュメント 967
詳細はこちら 969
AmazonOmicsFullAccess 969
このポリシーを使用すると 969
ポリシーの詳細 969
ポリシーのバージョン 969
JSON ポリシードキュメント 969
詳細はこちら 970
AmazonOmicsReadOnlyAccess 971
このポリシーを使用すると 971
ポリシーの詳細 971
ポリシーのバージョン 971
JSON ポリシードキュメント 971
詳細はこちら 972
AmazonOneEnterpriseFullAccess 972
このポリシーを使用すると 972
ポリシーの詳細 972
ポリシーのバージョン 972
JSON ポリシードキュメント 973
詳細はこちら 973

AmazonOneEnterpriseInstallerAccess 973
このポリシーを使用すると 973
ポリシーの詳細 973
ポリシーのバージョン 974
JSON ポリシードキュメント 974
詳細はこちら 974
AmazonOneEnterpriseReadOnlyAccess 975
このポリシーを使用すると 975
ポリシーの詳細 975
ポリシーのバージョン 975
JSON ポリシードキュメント 975
詳細はこちら 976
AmazonOpenSearchDashboardsServiceRolePolicy 976
このポリシーを使用すると 976
ポリシーの詳細 976
ポリシーのバージョン 976
JSON ポリシードキュメント 977
詳細はこちら 977
AmazonOpenSearchDirectQueryGlueCreateAccess 977
このポリシーを使用すると 977
ポリシーの詳細 978
ポリシーのバージョン 978
JSON ポリシードキュメント 978
詳細はこちら 978
AmazonOpenSearchIngestionFullAccess 979
このポリシーを使用すると 979
ポリシーの詳細 979
ポリシーのバージョン 979
JSON ポリシードキュメント 979
詳細はこちら 980
AmazonOpenSearchIngestionReadOnlyAccess 980
このポリシーを使用すると 981
ポリシーの詳細 981
ポリシーのバージョン 981
JSON ポリシードキュメント 981
詳細はこちら 982

AmazonOpenSearchIngestionServiceRolePolicy 982
このポリシーを使用すると 982
ポリシーの詳細 982
ポリシーのバージョン 982
JSON ポリシードキュメント 983
詳細はこちら 984
AmazonOpenSearchServerlessServiceRolePolicy 985
このポリシーを使用すると 985
ポリシーの詳細 985
ポリシーのバージョン 985
JSON ポリシードキュメント 985
詳細はこちら 986
AmazonOpenSearchServiceCognitoAccess 986
このポリシーを使用すると 986
ポリシーの詳細 986
ポリシーのバージョン 986
JSON ポリシードキュメント 987
詳細はこちら 988
AmazonOpenSearchServiceFullAccess 988
このポリシーを使用すると 988
ポリシーの詳細 988
ポリシーのバージョン 988
JSON ポリシードキュメント 989
詳細はこちら 989
AmazonOpenSearchServiceReadOnlyAccess 989
このポリシーを使用すると 989
ポリシーの詳細 990
ポリシーのバージョン 990
JSON ポリシードキュメント 990
詳細はこちら 990
AmazonOpenSearchServiceRolePolicy 991
このポリシーを使用すると 991
ポリシーの詳細 991
ポリシーのバージョン 991
JSON ポリシードキュメント 991
詳細はこちら 996

AmazonPersonalizeFullAccess 996
このポリシーを使用すると 996
ポリシーの詳細 997
ポリシーのバージョン 997
JSON ポリシードキュメント 997
詳細はこちら 998
AmazonPollyFullAccess 998
このポリシーを使用すると 998
ポリシーの詳細 999
ポリシーのバージョン 999
JSON ポリシードキュメント 999
詳細はこちら 999
AmazonPollyReadOnlyAccess 1000
このポリシーを使用すると 1000
ポリシーの詳細 1000
ポリシーのバージョン 1000
JSON ポリシードキュメント 1000
詳細はこちら 1001
AmazonPrometheusConsoleFullAccess 1001
このポリシーを使用すると 1001
ポリシーの詳細 1001
ポリシーのバージョン 1001
JSON ポリシードキュメント 1002
詳細はこちら 1003
AmazonPrometheusFullAccess 1003
このポリシーを使用すると 1003
ポリシーの詳細 1003
ポリシーのバージョン 1003
JSON ポリシードキュメント 1004
詳細はこちら 1005
AmazonPrometheusQueryAccess 1005
このポリシーを使用すると 1005
ポリシーの詳細 1005
ポリシーのバージョン 1005
JSON ポリシードキュメント 1006
詳細はこちら 1006

AmazonPrometheusRemoteWriteAccess 1006
このポリシーを使用すると 1006
ポリシーの詳細 1006
ポリシーのバージョン 1007
JSON ポリシードキュメント 1007
詳細はこちら 1007
AmazonPrometheusScraperServiceRolePolicy 1007
このポリシーを使用すると 1008
ポリシーの詳細 1008
ポリシーのバージョン 1008
JSON ポリシードキュメント 1008
詳細はこちら 1010
AmazonQDeveloperAccess 1011
このポリシーを使用すると 1011
ポリシーの詳細 1011
ポリシーのバージョン 1011
JSON ポリシードキュメント 1011
詳細はこちら 1012
AmazonQFullAccess 1013
このポリシーを使用すると 1013
ポリシーの詳細 1013
ポリシーのバージョン 1013
JSON ポリシードキュメント 1013
詳細はこちら 1015
AmazonQLDBConsoleFullAccess 1015
このポリシーを使用すると 1015
ポリシーの詳細 1015
ポリシーのバージョン 1016
JSON ポリシードキュメント 1016
詳細はこちら 1017
AmazonQLDBFullAccess 1018
このポリシーを使用すると 1018
ポリシーの詳細 1018
ポリシーのバージョン 1018
JSON ポリシードキュメント 1018
詳細はこちら 1020

AmazonQLDBReadOnly 1020
このポリシーを使用すると 1020
ポリシーの詳細 1020
ポリシーのバージョン 1020
JSON ポリシードキュメント 1020
詳細はこちら 1021
AmazonRDSBetaServiceRolePolicy 1021
このポリシーを使用すると 1021
ポリシーの詳細 1022
ポリシーのバージョン 1022
JSON ポリシードキュメント 1022
詳細はこちら 1025
AmazonRDSCustomInstanceProfileRolePolicy 1025
このポリシーを使用すると 1025
ポリシーの詳細 1025
ポリシーのバージョン 1026
JSON ポリシードキュメント 1026
詳細はこちら 1033
AmazonRDSCustomPreviewServiceRolePolicy 1033
このポリシーを使用すると 1033
ポリシーの詳細 1033
ポリシーのバージョン 1034
JSON ポリシードキュメント 1034
詳細はこちら 1051
AmazonRDSCustomServiceRolePolicy 1052
このポリシーを使用すると 1052
ポリシーの詳細 1052
ポリシーのバージョン 1052
JSON ポリシードキュメント 1052
詳細はこちら 1071
AmazonRDSDataFullAccess 1071
このポリシーを使用すると 1071
ポリシーの詳細 1072
ポリシーのバージョン 1072
JSON ポリシードキュメント 1072
詳細はこちら 1073

AmazonRDSDirectoryServiceAccess 1073
このポリシーを使用すると 1073
ポリシーの詳細 1074
ポリシーのバージョン 1074
JSON ポリシードキュメント 1074
詳細はこちら 1074
AmazonRDSEnhancedMonitoringRole 1075
このポリシーを使用すると 1075
ポリシーの詳細 1075
ポリシーのバージョン 1075
JSON ポリシードキュメント 1075
詳細はこちら 1076
AmazonRDSFullAccess 1076
このポリシーを使用すると 1076
ポリシーの詳細 1077
ポリシーのバージョン 1077
JSON ポリシードキュメント 1077
詳細はこちら 1079
AmazonRDSPerformanceInsightsFullAccess 1079
このポリシーを使用すると 1079
ポリシーの詳細 1079
ポリシーのバージョン 1080
JSON ポリシードキュメント 1080
詳細はこちら 1081
AmazonRDSPerformanceInsightsReadOnly 1082
このポリシーを使用すると 1082
ポリシーの詳細 1082
ポリシーのバージョン 1082
JSON ポリシードキュメント 1082
詳細はこちら 1084
AmazonRDSPreviewServiceRolePolicy 1085
このポリシーを使用すると 1085
ポリシーの詳細 1085
ポリシーのバージョン 1085
JSON ポリシードキュメント 1085
詳細はこちら 1088

AmazonRDSReadOnlyAccess 1088
このポリシーを使用すると 1089
ポリシーの詳細 1089
ポリシーのバージョン 1089
JSON ポリシードキュメント 1089
詳細はこちら 1090
AmazonRDSServiceRolePolicy 1091
このポリシーを使用すると 1091
ポリシーの詳細 1091
ポリシーのバージョン 1091
JSON ポリシードキュメント 1091
詳細はこちら 1095
AmazonRedshiftAllCommandsFullAccess 1095
このポリシーを使用すると 1095
ポリシーの詳細 1095
ポリシーのバージョン 1096
JSON ポリシードキュメント 1096
詳細はこちら 1101
AmazonRedshiftDataFullAccess 1101
このポリシーを使用すると 1101
ポリシーの詳細 1102
ポリシーのバージョン 1102
JSON ポリシードキュメント 1102
詳細はこちら 1104
AmazonRedshiftFederatedAuthorization 1104
このポリシーを使用すると 1104
ポリシーの詳細 1104
ポリシーのバージョン 1105
JSON ポリシードキュメント 1105
詳細はこちら 1106
AmazonRedshiftFullAccess 1106
このポリシーを使用すると 1106
ポリシーの詳細 1106
ポリシーのバージョン 1107
JSON ポリシードキュメント 1107
詳細はこちら 1109

AmazonRedshiftQueryEditor 1109
このポリシーを使用すると 1109
ポリシーの詳細 1109
ポリシーのバージョン 1109
JSON ポリシードキュメント 1110
詳細はこちら 1112
AmazonRedshiftQueryEditorV2FullAccess 1112
このポリシーを使用すると 1112
ポリシーの詳細 1112
ポリシーのバージョン 1112
JSON ポリシードキュメント 1113
詳細はこちら 1114
AmazonRedshiftQueryEditorV2NoSharing 1114
このポリシーを使用すると 1114
ポリシーの詳細 1114
ポリシーのバージョン 1115
JSON ポリシードキュメント 1115
詳細はこちら 1118
AmazonRedshiftQueryEditorV2ReadSharing 1119
このポリシーを使用すると 1119
ポリシーの詳細 1119
ポリシーのバージョン 1119
JSON ポリシードキュメント 1119
詳細はこちら 1124
AmazonRedshiftQueryEditorV2ReadWriteSharing 1125
このポリシーを使用すると 1125
ポリシーの詳細 1125
ポリシーのバージョン 1125
JSON ポリシードキュメント 1125
詳細はこちら 1130
AmazonRedshiftReadOnlyAccess 1131
このポリシーを使用すると 1131
ポリシーの詳細 1131
ポリシーのバージョン 1131
JSON ポリシードキュメント 1131
詳細はこちら 1132

AmazonRedshiftServiceLinkedRolePolicy 1132
このポリシーを使用すると 1132
ポリシーの詳細 1132
ポリシーのバージョン 1133
JSON ポリシードキュメント 1133
詳細はこちら 1139
AmazonRekognitionCustomLabelsFullAccess 1139
このポリシーを使用すると 1139
ポリシーの詳細 1140
ポリシーのバージョン 1140
JSON ポリシードキュメント 1140
詳細はこちら 1141
AmazonRekognitionFullAccess 1141
このポリシーを使用すると 1142
ポリシーの詳細 1142
ポリシーのバージョン 1142
JSON ポリシードキュメント 1142
詳細はこちら 1142
AmazonRekognitionReadOnlyAccess 1143
このポリシーを使用すると 1143
ポリシーの詳細 1143
ポリシーのバージョン 1143
JSON ポリシードキュメント 1143
詳細はこちら 1144
AmazonRekognitionServiceRole 1145
このポリシーを使用すると 1145
ポリシーの詳細 1145
ポリシーのバージョン 1145
JSON ポリシードキュメント 1145
詳細はこちら 1146
AmazonRoute53AutoNamingFullAccess 1146
このポリシーを使用すると 1146
ポリシーの詳細 1147
ポリシーのバージョン 1147
JSON ポリシードキュメント 1147
詳細はこちら 1148

AmazonRoute53AutoNamingReadOnlyAccess 1148
このポリシーを使用すると 1148
ポリシーの詳細 1148
ポリシーのバージョン 1148
JSON ポリシードキュメント 1149
詳細はこちら 1149
AmazonRoute53AutoNamingRegistrantAccess 1149
このポリシーを使用すると 1149
ポリシーの詳細 1149
ポリシーのバージョン 1150
JSON ポリシードキュメント 1150
詳細はこちら 1151
AmazonRoute53DomainsFullAccess 1151
このポリシーを使用すると 1151
ポリシーの詳細 1151
ポリシーのバージョン 1151
JSON ポリシードキュメント 1151
詳細はこちら 1152
AmazonRoute53DomainsReadOnlyAccess 1152
このポリシーを使用すると 1152
ポリシーの詳細 1152
ポリシーのバージョン 1153
JSON ポリシードキュメント 1153
詳細はこちら 1153
AmazonRoute53FullAccess 1153
このポリシーを使用すると 1154
ポリシーの詳細 1154
ポリシーのバージョン 1154
JSON ポリシードキュメント 1154
詳細はこちら 1155
AmazonRoute53ProfilesFullAccess 1155
このポリシーを使用すると 1155
ポリシーの詳細 1156
ポリシーのバージョン 1156
JSON ポリシードキュメント 1156
詳細はこちら 1157

AmazonRoute53ProfilesReadOnlyAccess 1157
このポリシーを使用すると 1157
ポリシーの詳細 1157
ポリシーのバージョン 1158
JSON ポリシードキュメント 1158
詳細はこちら 1159
AmazonRoute53ReadOnlyAccess 1159
このポリシーを使用すると 1159
ポリシーの詳細 1159
ポリシーのバージョン 1159
JSON ポリシードキュメント 1159
詳細はこちら 1160
AmazonRoute53RecoveryClusterFullAccess 1160
このポリシーを使用すると 1160
ポリシーの詳細 1160
ポリシーのバージョン 1161
JSON ポリシードキュメント 1161
詳細はこちら 1161
AmazonRoute53RecoveryClusterReadOnlyAccess 1161
このポリシーを使用すると 1162
ポリシーの詳細 1162
ポリシーのバージョン 1162
JSON ポリシードキュメント 1162
詳細はこちら 1162
AmazonRoute53RecoveryControlConfigFullAccess 1163
このポリシーを使用すると 1163
ポリシーの詳細 1163
ポリシーのバージョン 1163
JSON ポリシードキュメント 1163
詳細はこちら 1164
AmazonRoute53RecoveryControlConfigReadOnlyAccess 1164
このポリシーを使用すると 1164
ポリシーの詳細 1164
ポリシーのバージョン 1164
JSON ポリシードキュメント 1165
詳細はこちら 1165

AmazonRoute53RecoveryReadinessFullAccess 1165
このポリシーを使用すると 1166
ポリシーの詳細 1166
ポリシーのバージョン 1166
JSON ポリシードキュメント 1166
詳細はこちら 1167
AmazonRoute53RecoveryReadinessReadOnlyAccess 1167
このポリシーを使用すると 1167
ポリシーの詳細 1167
ポリシーのバージョン 1167
JSON ポリシードキュメント 1167
詳細はこちら 1168
AmazonRoute53ResolverFullAccess 1169
このポリシーを使用すると 1169
ポリシーの詳細 1169
ポリシーのバージョン 1169
JSON ポリシードキュメント 1169
詳細はこちら 1170
AmazonRoute53ResolverReadOnlyAccess 1170
このポリシーを使用すると 1170
ポリシーの詳細 1170
ポリシーのバージョン 1171
JSON ポリシードキュメント 1171
詳細はこちら 1171
AmazonS3FullAccess 1172
このポリシーを使用すると 1172
ポリシーの詳細 1172
ポリシーのバージョン 1172
JSON ポリシードキュメント 1172
詳細はこちら 1173
AmazonS3ObjectLambdaExecutionRolePolicy 1173
このポリシーを使用すると 1173
ポリシーの詳細 1173
ポリシーのバージョン 1173
JSON ポリシードキュメント 1174
詳細はこちら 1174

AmazonS3OutpostsFullAccess 1174
このポリシーを使用すると 1174
ポリシーの詳細 1174
ポリシーのバージョン 1175
JSON ポリシードキュメント 1175
詳細はこちら 1176
AmazonS3OutpostsReadOnlyAccess 1176
このポリシーを使用すると 1176
ポリシーの詳細 1176
ポリシーのバージョン 1177
JSON ポリシードキュメント 1177
詳細はこちら 1178
AmazonS3ReadOnlyAccess 1178
このポリシーを使用すると 1178
ポリシーの詳細 1178
ポリシーのバージョン 1178
JSON ポリシードキュメント 1179
詳細はこちら 1179
AmazonS3TablesFullAccess 1179
このポリシーを使用すると 1179
ポリシーの詳細 1180
ポリシーのバージョン 1180
JSON ポリシードキュメント 1180
詳細はこちら 1181
AmazonS3TablesLakeFormationServiceRole 1181
このポリシーを使用すると 1181
ポリシーの詳細 1181
ポリシーのバージョン 1181
JSON ポリシードキュメント 1182
詳細はこちら 1184
AmazonS3TablesReadOnlyAccess 1184
このポリシーを使用すると 1184
ポリシーの詳細 1184
ポリシーのバージョン 1184
JSON ポリシードキュメント 1185
詳細はこちら 1185

AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy 1185
このポリシーを使用すると 1186
ポリシーの詳細 1186
ポリシーのバージョン 1186
JSON ポリシードキュメント 1186
詳細はこちら 1197
AmazonSageMakerCanvasAIServicesAccess 1198
このポリシーを使用すると 1198
ポリシーの詳細 1198
ポリシーのバージョン 1198
JSON ポリシードキュメント 1198
詳細はこちら 1201
AmazonSageMakerCanvasBedrockAccess 1202
このポリシーを使用すると 1202
ポリシーの詳細 1202
ポリシーのバージョン 1202
JSON ポリシードキュメント 1202
詳細はこちら 1203
AmazonSageMakerCanvasDataPrepFullAccess 1203
このポリシーを使用すると 1203
ポリシーの詳細 1204
ポリシーのバージョン 1204
JSON ポリシードキュメント 1204
詳細はこちら 1213
AmazonSageMakerCanvasDirectDeployAccess 1214
このポリシーを使用すると 1214
ポリシーの詳細 1214
ポリシーのバージョン 1214
JSON ポリシードキュメント 1214
詳細はこちら 1215
AmazonSageMakerCanvasEMRServerlessExecutionRolePolicy 1215
このポリシーを使用すると 1215
ポリシーの詳細 1216
ポリシーのバージョン 1216
JSON ポリシードキュメント 1216
詳細はこちら 1217

AmazonSageMakerCanvasForecastAccess 1218
このポリシーを使用すると 1218
ポリシーの詳細 1218
ポリシーのバージョン 1218
JSON ポリシードキュメント 1218
詳細はこちら 1219
AmazonSageMakerCanvasFullAccess 1219
このポリシーを使用すると 1219
ポリシーの詳細 1220
ポリシーのバージョン 1220
JSON ポリシードキュメント 1220
詳細はこちら 1232
AmazonSageMakerCanvasSMDataScienceAssistantAccess 1232
このポリシーを使用すると 1233
ポリシーの詳細 1233
ポリシーのバージョン 1233
JSON ポリシードキュメント 1233
詳細はこちら 1234
AmazonSageMakerClusterInstanceRolePolicy 1234
このポリシーを使用すると 1234
ポリシーの詳細 1234
ポリシーのバージョン 1235
JSON ポリシードキュメント 1235
詳細はこちら 1237
AmazonSageMakerCoreServiceRolePolicy 1237
このポリシーを使用すると 1237
ポリシーの詳細 1237
ポリシーのバージョン 1237
JSON ポリシードキュメント 1238
詳細はこちら 1239
AmazonSageMakerEdgeDeviceFleetPolicy 1239
このポリシーを使用すると 1239
ポリシーの詳細 1239
ポリシーのバージョン 1239
JSON ポリシードキュメント 1239
詳細はこちら 1241

AmazonSageMakerFeatureStoreAccess 1241
このポリシーを使用すると 1242
ポリシーの詳細 1242
ポリシーのバージョン 1242
JSON ポリシードキュメント 1242
詳細はこちら 1243
AmazonSageMakerFullAccess 1243
このポリシーを使用すると 1244
ポリシーの詳細 1244
ポリシーのバージョン 1244
JSON ポリシードキュメント 1244
詳細はこちら 1260
AmazonSageMakerGeospatialExecutionRole 1261
このポリシーを使用すると 1261
ポリシーの詳細 1261
ポリシーのバージョン 1261
JSON ポリシードキュメント 1261
詳細はこちら 1262
AmazonSageMakerGeospatialFullAccess 1262
このポリシーを使用すると 1262
ポリシーの詳細 1263
ポリシーのバージョン 1263
JSON ポリシードキュメント 1263
詳細はこちら 1264
AmazonSageMakerGroundTruthExecution 1264
このポリシーを使用すると 1264
ポリシーの詳細 1264
ポリシーのバージョン 1264
JSON ポリシードキュメント 1265
詳細はこちら 1268
AmazonSageMakerHyperPodObservabilityAdminAccess 1268
このポリシーを使用すると 1268
ポリシーの詳細 1269
ポリシーのバージョン 1269
JSON ポリシードキュメント 1269
詳細はこちら 1275

AmazonSageMakerHyperPodServiceRolePolicy 1276
このポリシーを使用すると 1276
ポリシーの詳細 1276
ポリシーのバージョン 1276
JSON ポリシードキュメント 1276
詳細はこちら 1277
AmazonSageMakerHyperPodTrainingOperatorAccess 1278
このポリシーを使用すると 1278
ポリシーの詳細 1278
ポリシーのバージョン 1278
JSON ポリシードキュメント 1278
詳細はこちら 1279
AmazonSageMakerMechanicalTurkAccess 1279
このポリシーを使用すると 1279
ポリシーの詳細 1279
ポリシーのバージョン 1280
JSON ポリシードキュメント 1280
詳細はこちら 1280
AmazonSageMakerModelGovernanceUseAccess 1280
このポリシーを使用すると 1281
ポリシーの詳細 1281
ポリシーのバージョン 1281
JSON ポリシードキュメント 1281
詳細はこちら 1283
AmazonSageMakerModelRegistryFullAccess 1283
このポリシーを使用すると 1283
ポリシーの詳細 1283
ポリシーのバージョン 1284
JSON ポリシードキュメント 1284
詳細はこちら 1287
AmazonSageMakerNotebooksServiceRolePolicy 1288
このポリシーを使用すると 1288
ポリシーの詳細 1288
ポリシーのバージョン 1288
JSON ポリシードキュメント 1288
詳細はこちら 1293

AmazonSageMakerPartnerAppsFullAccess 1294
このポリシーを使用すると 1294
ポリシーの詳細 1294
ポリシーのバージョン 1294
JSON ポリシードキュメント 1294
詳細はこちら 1295
AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy 1295
このポリシーを使用すると 1295
ポリシーの詳細 1296
ポリシーのバージョン 1296
JSON ポリシードキュメント 1296
詳細はこちら 1297
AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy 1297
このポリシーを使用すると 1297
ポリシーの詳細 1297
ポリシーのバージョン 1298
JSON ポリシードキュメント 1298
詳細はこちら 1301
AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy 1302
このポリシーを使用すると 1302
ポリシーの詳細 1302
ポリシーのバージョン 1302
JSON ポリシードキュメント 1302
詳細はこちら 1303
AmazonSageMakerPipelinesIntegrations 1303
このポリシーを使用すると 1303
ポリシーの詳細 1303
ポリシーのバージョン 1304
JSON ポリシードキュメント 1304
詳細はこちら 1306
AmazonSageMakerQuickSightVPCPolicy 1306
このポリシーを使用すると 1306
ポリシーの詳細 1306
ポリシーのバージョン 1306
JSON ポリシードキュメント 1307
詳細はこちら 1308

AmazonSageMakerReadOnly 1308
このポリシーを使用すると 1308
ポリシーの詳細 1309
ポリシーのバージョン 1309
JSON ポリシードキュメント 1309
詳細はこちら 1310
AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy 1310
このポリシーを使用すると 1311
ポリシーの詳細 1311
ポリシーのバージョン 1311
JSON ポリシードキュメント 1311
詳細はこちら 1312
AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy 1312
このポリシーを使用すると 1312
ポリシーの詳細 1312
ポリシーのバージョン 1313
JSON ポリシードキュメント 1313
詳細はこちら 1320
AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy 1320
このポリシーを使用すると 1320
ポリシーの詳細 1320
ポリシーのバージョン 1320
JSON ポリシードキュメント 1321
詳細はこちら 1331
AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy 1331
このポリシーを使用すると 1331
ポリシーの詳細 1331
ポリシーのバージョン 1332
JSON ポリシードキュメント 1332
詳細はこちら 1335
AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy 1335
このポリシーを使用すると 1335
ポリシーの詳細 1335
ポリシーのバージョン 1335
JSON ポリシードキュメント 1336
詳細はこちら 1336

AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy 1336
このポリシーを使用すると 1336
ポリシーの詳細 1336
ポリシーのバージョン 1337
JSON ポリシードキュメント 1337
詳細はこちら 1337
AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy 1338
このポリシーを使用すると 1338
ポリシーの詳細 1338
ポリシーのバージョン 1338
JSON ポリシードキュメント 1338
詳細はこちら 1340
AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy 1341
このポリシーを使用すると 1341
ポリシーの詳細 1341
ポリシーのバージョン 1341
JSON ポリシードキュメント 1342
詳細はこちら 1352
AmazonSageMakerSpacesControllerPolicy 1352
このポリシーを使用すると 1352
ポリシーの詳細 1352
ポリシーのバージョン 1352
JSON ポリシードキュメント 1353
詳細はこちら 1357
AmazonSageMakerSpacesRouterPolicy 1357
このポリシーを使用すると 1358
ポリシーの詳細 1358
ポリシーのバージョン 1358
JSON ポリシードキュメント 1358
詳細はこちら 1359
AmazonSageMakerTrainingPlanCreateAccess 1359
このポリシーを使用すると 1359
ポリシーの詳細 1359
ポリシーのバージョン 1360
JSON ポリシードキュメント 1360
詳細はこちら 1361

AmazonSecurityLakeAdministrator 1362
このポリシーを使用すると 1362
ポリシーの詳細 1362
ポリシーのバージョン 1362
JSON ポリシードキュメント 1362
詳細はこちら 1373
AmazonSecurityLakeMetastoreManager 1374
このポリシーを使用すると 1374
ポリシーの詳細 1374
ポリシーのバージョン 1374
JSON ポリシードキュメント 1374
詳細はこちら 1377
AmazonSecurityLakePermissionsBoundary 1377
このポリシーを使用すると 1377
ポリシーの詳細 1377
ポリシーのバージョン 1377
JSON ポリシードキュメント 1378
詳細はこちら 1381
AmazonSESFullAccess 1381
このポリシーを使用すると 1381
ポリシーの詳細 1381
ポリシーのバージョン 1381
JSON ポリシードキュメント 1382
詳細はこちら 1382
AmazonSESReadOnlyAccess 1382
このポリシーを使用すると 1382
ポリシーの詳細 1382
ポリシーのバージョン 1383
JSON ポリシードキュメント 1383
詳細はこちら 1383
AmazonSESServiceRolePolicy 1383
このポリシーを使用すると 1384
ポリシーの詳細 1384
ポリシーのバージョン 1384
JSON ポリシードキュメント 1384
詳細はこちら 1385

AmazonSNSFullAccess 1385
このポリシーを使用すると 1385
ポリシーの詳細 1385
ポリシーのバージョン 1385
JSON ポリシードキュメント 1385
詳細はこちら 1386
AmazonSNSReadOnlyAccess 1387
このポリシーを使用すると 1387
ポリシーの詳細 1387
ポリシーのバージョン 1387
JSON ポリシードキュメント 1387
詳細はこちら 1388
AmazonSNSRole 1388
このポリシーを使用すると 1389
ポリシーの詳細 1389
ポリシーのバージョン 1389
JSON ポリシードキュメント 1389
詳細はこちら 1390
AmazonSQSFullAccess 1390
このポリシーを使用すると 1390
ポリシーの詳細 1390
ポリシーのバージョン 1390
JSON ポリシードキュメント 1390
詳細はこちら 1391
AmazonSQSReadOnlyAccess 1391
このポリシーを使用すると 1391
ポリシーの詳細 1391
ポリシーのバージョン 1391
JSON ポリシードキュメント 1392
詳細はこちら 1392
AmazonSSMAutomationApproverAccess 1392
このポリシーを使用すると 1393
ポリシーの詳細 1393
ポリシーのバージョン 1393
JSON ポリシードキュメント 1393
詳細はこちら 1394

AmazonSSMAutomationRole 1394
このポリシーを使用すると 1394
ポリシーの詳細 1394
ポリシーのバージョン 1394
JSON ポリシードキュメント 1394
詳細はこちら 1396
AmazonSSMDirectoryServiceAccess 1396
このポリシーを使用すると 1396
ポリシーの詳細 1397
ポリシーのバージョン 1397
JSON ポリシードキュメント 1397
詳細はこちら 1397
AmazonSSMFullAccess 1398
このポリシーを使用すると 1398
ポリシーの詳細 1398
ポリシーのバージョン 1398
JSON ポリシードキュメント 1398
詳細はこちら 1399
AmazonSSMMaintenanceWindowRole 1400
このポリシーを使用すると 1400
ポリシーの詳細 1400
ポリシーのバージョン 1400
JSON ポリシードキュメント 1400
詳細はこちら 1402
AmazonSSMManagedEC2InstanceDefaultPolicy 1402
このポリシーを使用すると 1402
ポリシーの詳細 1402
ポリシーのバージョン 1402
JSON ポリシードキュメント 1403
詳細はこちら 1404
AmazonSSMManagedInstanceCore 1404
このポリシーを使用すると 1404
ポリシーの詳細 1404
ポリシーのバージョン 1404
JSON ポリシードキュメント 1405
詳細はこちら 1406

AmazonSSMPatchAssociation 1406
このポリシーを使用すると 1406
ポリシーの詳細 1406
ポリシーのバージョン 1407
JSON ポリシードキュメント 1407
詳細はこちら 1407
AmazonSSMReadOnlyAccess 1408
このポリシーを使用すると 1408
ポリシーの詳細 1408
ポリシーのバージョン 1408
JSON ポリシードキュメント 1408
詳細はこちら 1409
AmazonSSMServiceRolePolicy 1409
このポリシーを使用すると 1409
ポリシーの詳細 1409
ポリシーのバージョン 1409
JSON ポリシードキュメント 1410
詳細はこちら 1415
AmazonSumerianFullAccess 1415
このポリシーを使用すると 1416
ポリシーの詳細 1416
ポリシーのバージョン 1416
JSON ポリシードキュメント 1416
詳細はこちら 1416
AmazonTextractFullAccess 1417
このポリシーを使用すると 1417
ポリシーの詳細 1417
ポリシーのバージョン 1417
JSON ポリシードキュメント 1417
詳細はこちら 1418
AmazonTextractServiceRole 1418
このポリシーを使用すると 1418
ポリシーの詳細 1418
ポリシーのバージョン 1418
JSON ポリシードキュメント 1419
詳細はこちら 1419

AmazonTimestreamConsoleFullAccess 1419
このポリシーを使用すると 1419
ポリシーの詳細 1419
ポリシーのバージョン 1420
JSON ポリシードキュメント 1420
詳細はこちら 1423
AmazonTimestreamFullAccess 1423
このポリシーを使用すると 1423
ポリシーの詳細 1423
ポリシーのバージョン 1423
JSON ポリシードキュメント 1423
詳細はこちら 1425
AmazonTimestreamInfluxDBFullAccess 1425
このポリシーを使用すると 1425
ポリシーの詳細 1425
ポリシーのバージョン 1425
JSON ポリシードキュメント 1426
詳細はこちら 1428
AmazonTimestreamInfluxDBFullAccessWithoutMarketplaceAccess 1428
このポリシーを使用すると 1429
ポリシーの詳細 1429
ポリシーのバージョン 1429
JSON ポリシードキュメント 1429
詳細はこちら 1431
AmazonTimestreamInfluxDBServiceRolePolicy 1431
このポリシーを使用すると 1432
ポリシーの詳細 1432
ポリシーのバージョン 1432
JSON ポリシードキュメント 1432
詳細はこちら 1435
AmazonTimestreamReadOnlyAccess 1435
このポリシーを使用すると 1435
ポリシーの詳細 1435
ポリシーのバージョン 1435
JSON ポリシードキュメント 1436
詳細はこちら 1436

AmazonTranscribeFullAccess 1436
このポリシーを使用すると 1437
ポリシーの詳細 1437
ポリシーのバージョン 1437
JSON ポリシードキュメント 1437
詳細はこちら 1438
AmazonTranscribeReadOnlyAccess 1438
このポリシーを使用すると 1438
ポリシーの詳細 1438
ポリシーのバージョン 1438
JSON ポリシードキュメント 1439
詳細はこちら 1439
AmazonVerifiedPermissionsFullAccess 1439
このポリシーを使用すると 1439
ポリシーの詳細 1439
ポリシーのバージョン 1440
JSON ポリシードキュメント 1440
詳細はこちら 1440
AmazonVerifiedPermissionsReadOnlyAccess 1441
このポリシーを使用すると 1441
ポリシーの詳細 1441
ポリシーのバージョン 1441
JSON ポリシードキュメント 1441
詳細はこちら 1442
AmazonVPCCrossAccountNetworkInterfaceOperations 1442
このポリシーを使用すると 1443
ポリシーの詳細 1443
ポリシーのバージョン 1443
JSON ポリシードキュメント 1443
詳細はこちら 1445
AmazonVPCFullAccess 1445
このポリシーを使用すると 1445
ポリシーの詳細 1445
ポリシーのバージョン 1445
JSON ポリシードキュメント 1445
詳細はこちら 1449

AmazonVPCNetworkAccessAnalyzerFullAccessPolicy 1450
このポリシーを使用すると 1450
ポリシーの詳細 1450
ポリシーのバージョン 1450
JSON ポリシードキュメント 1450
詳細はこちら 1454
AmazonVPCReachabilityAnalyzerFullAccessPolicy 1454
このポリシーを使用すると 1454
ポリシーの詳細 1454
ポリシーのバージョン 1454
JSON ポリシードキュメント 1455
詳細はこちら 1458
AmazonVPCReachabilityAnalyzerPathComponentReadPolicy 1458
このポリシーを使用すると 1458
ポリシーの詳細 1458
ポリシーのバージョン 1458
JSON ポリシードキュメント 1459
詳細はこちら 1459
AmazonVPCReadOnlyAccess 1459
このポリシーを使用すると 1459
ポリシーの詳細 1459
ポリシーのバージョン 1460
JSON ポリシードキュメント 1460
詳細はこちら 1461
AmazonWorkDocsFullAccess 1461
このポリシーを使用すると 1461
ポリシーの詳細 1462
ポリシーのバージョン 1462
JSON ポリシードキュメント 1462
詳細はこちら 1462
AmazonWorkDocsReadOnlyAccess 1463
このポリシーを使用すると 1463
ポリシーの詳細 1463
ポリシーのバージョン 1463
JSON ポリシードキュメント 1463
詳細はこちら 1464

AmazonWorkMailEventsServiceRolePolicy 1464
このポリシーを使用すると 1464
ポリシーの詳細 1464
ポリシーのバージョン 1465
JSON ポリシードキュメント 1465
詳細はこちら 1465
AmazonWorkMailFullAccess 1465
このポリシーを使用すると 1465
ポリシーの詳細 1466
ポリシーのバージョン 1466
JSON ポリシードキュメント 1466
詳細はこちら 1468
AmazonWorkMailMessageFlowFullAccess 1468
このポリシーを使用すると 1468
ポリシーの詳細 1468
ポリシーのバージョン 1469
JSON ポリシードキュメント 1469
詳細はこちら 1469
AmazonWorkMailMessageFlowReadOnlyAccess 1469
このポリシーを使用すると 1470
ポリシーの詳細 1470
ポリシーのバージョン 1470
JSON ポリシードキュメント 1470
詳細はこちら 1470
AmazonWorkMailReadOnlyAccess 1471
このポリシーを使用すると 1471
ポリシーの詳細 1471
ポリシーのバージョン 1471
JSON ポリシードキュメント 1471
詳細はこちら 1472
AmazonWorkSpacesAdmin 1472
このポリシーを使用すると 1472
ポリシーの詳細 1472
ポリシーのバージョン 1473
JSON ポリシードキュメント 1473
詳細はこちら 1474

AmazonWorkSpacesApplicationManagerAdminAccess 1474
このポリシーを使用すると 1474
ポリシーの詳細 1474
ポリシーのバージョン 1475
JSON ポリシードキュメント 1475
詳細はこちら 1475
AmazonWorkspacesPCAAccess 1475
このポリシーを使用すると 1476
ポリシーの詳細 1476
ポリシーのバージョン 1476
JSON ポリシードキュメント 1476
詳細はこちら 1477
AmazonWorkSpacesPoolServiceAccess 1477
このポリシーを使用すると 1477
ポリシーの詳細 1477
ポリシーのバージョン 1477
JSON ポリシードキュメント 1478
詳細はこちら 1479
AmazonWorkSpacesSecureBrowserReadOnly 1479
このポリシーを使用すると 1479
ポリシーの詳細 1479
ポリシーのバージョン 1479
JSON ポリシードキュメント 1480
詳細はこちら 1481
AmazonWorkSpacesSelfServiceAccess 1481
このポリシーを使用すると 1481
ポリシーの詳細 1481
ポリシーのバージョン 1481
JSON ポリシードキュメント 1482
詳細はこちら 1482
AmazonWorkSpacesServiceAccess 1482
このポリシーを使用すると 1482
ポリシーの詳細 1483
ポリシーのバージョン 1483
JSON ポリシードキュメント 1483
詳細はこちら 1483

AmazonWorkSpacesThinClientFullAccess 1484
このポリシーを使用すると 1484
ポリシーの詳細 1484
ポリシーのバージョン 1484
JSON ポリシードキュメント 1484
詳細はこちら 1486
AmazonWorkSpacesThinClientMonitoringServiceRolePolicy 1486
このポリシーを使用すると 1486
ポリシーの詳細 1486
ポリシーのバージョン 1486
JSON ポリシードキュメント 1487
詳細はこちら 1487
AmazonWorkSpacesThinClientReadOnlyAccess 1487
このポリシーを使用すると 1487
ポリシーの詳細 1488
ポリシーのバージョン 1488
JSON ポリシードキュメント 1488
詳細はこちら 1489
AmazonWorkSpacesWebReadOnly 1489
このポリシーを使用すると 1490
ポリシーの詳細 1490
ポリシーのバージョン 1490
JSON ポリシードキュメント 1490
詳細はこちら 1491
AmazonWorkSpacesWebServiceRolePolicy 1491
このポリシーを使用すると 1491
ポリシーの詳細 1492
ポリシーのバージョン 1492
JSON ポリシードキュメント 1492
詳細はこちら 1494
AmazonZocaloFullAccess 1494
このポリシーを使用すると 1495
ポリシーの詳細 1495
ポリシーのバージョン 1495
JSON ポリシードキュメント 1495
詳細はこちら 1496

AmazonZocaloReadOnlyAccess 1496
このポリシーを使用すると 1496
ポリシーの詳細 1496
ポリシーのバージョン 1496
JSON ポリシードキュメント 1497
詳細はこちら 1497
AmplifyBackendDeployFullAccess 1497
このポリシーを使用すると 1498
ポリシーの詳細 1498
ポリシーのバージョン 1498
JSON ポリシードキュメント 1498
詳細はこちら 1502
APIGatewayServiceRolePolicy 1503
このポリシーを使用すると 1503
ポリシーの詳細 1503
ポリシーのバージョン 1503
JSON ポリシードキュメント 1503
詳細はこちら 1505
AppIntegrationsServiceLinkedRolePolicy 1506
このポリシーを使用すると 1506
ポリシーの詳細 1506
ポリシーのバージョン 1506
JSON ポリシードキュメント 1506
詳細はこちら 1508
ApplicationAutoScalingForAmazonAppStreamAccess 1508
このポリシーを使用すると 1508
ポリシーの詳細 1508
ポリシーのバージョン 1509
JSON ポリシードキュメント 1509
詳細はこちら 1509
ApplicationDiscoveryServiceContinuousExportServiceRolePolicy 1510
このポリシーを使用すると 1510
ポリシーの詳細 1510
ポリシーのバージョン 1510
JSON ポリシードキュメント 1510
詳細はこちら 1512

AppRunnerNetworkingServiceRolePolicy 1512
このポリシーを使用すると 1513
ポリシーの詳細 1513
ポリシーのバージョン 1513
JSON ポリシードキュメント 1513
詳細はこちら 1514
AppRunnerServiceRolePolicy 1515
このポリシーを使用すると 1515
ポリシーの詳細 1515
ポリシーのバージョン 1515
JSON ポリシードキュメント 1515
詳細はこちら 1516
AppStudioServiceRolePolicy 1516
このポリシーを使用すると 1517
ポリシーの詳細 1517
ポリシーのバージョン 1517
JSON ポリシードキュメント 1517
詳細はこちら 1519
AuroraDsqlServiceLinkedRolePolicy 1519
このポリシーを使用すると 1520
ポリシーの詳細 1520
ポリシーのバージョン 1520
JSON ポリシードキュメント 1520
詳細はこちら 1521
AutoScalingConsoleFullAccess 1521
このポリシーを使用すると 1521
ポリシーの詳細 1521
ポリシーのバージョン 1521
JSON ポリシードキュメント 1522
詳細はこちら 1523
AutoScalingConsoleReadOnlyAccess 1523
このポリシーを使用すると 1524
ポリシーの詳細 1524
ポリシーのバージョン 1524
JSON ポリシードキュメント 1524
詳細はこちら 1525

AutoScalingFullAccess 1525
このポリシーを使用すると 1526
ポリシーの詳細 1526
ポリシーのバージョン 1526
JSON ポリシードキュメント 1526
詳細はこちら 1527
AutoScalingNotificationAccessRole 1528
このポリシーを使用すると 1528
ポリシーの詳細 1528
ポリシーのバージョン 1528
JSON ポリシードキュメント 1528
詳細はこちら 1529
AutoScalingReadOnlyAccess 1529
このポリシーを使用すると 1529
ポリシーの詳細 1529
ポリシーのバージョン 1529
JSON ポリシードキュメント 1530
詳細はこちら 1530
AutoScalingServiceRolePolicy 1530
このポリシーを使用すると 1530
ポリシーの詳細 1530
ポリシーのバージョン 1531
JSON ポリシードキュメント 1531
詳細はこちら 1534
AWS-SSM-Automation-DiagnosisBucketPolicy 1534
このポリシーを使用すると 1534
ポリシーの詳細 1534
ポリシーのバージョン 1534
JSON ポリシードキュメント 1535
詳細はこちら 1537
AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy 1537
このポリシーを使用すると 1537
ポリシーの詳細 1538
ポリシーのバージョン 1538
JSON ポリシードキュメント 1538
詳細はこちら 1540

AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy 1541
このポリシーを使用すると 1541
ポリシーの詳細 1541
ポリシーのバージョン 1541
JSON ポリシードキュメント 1541
詳細はこちら 1543
AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrationRolePolicy 1543
このポリシーを使用すると 1544
ポリシーの詳細 1544
ポリシーのバージョン 1544
JSON ポリシードキュメント 1544
詳細はこちら 1545
AWS-SSM-RemediationAutomation-AdministrationRolePolicy 1545
このポリシーを使用すると 1545
ポリシーの詳細 1546
ポリシーのバージョン 1546
JSON ポリシードキュメント 1546
詳細はこちら 1548
AWS-SSM-RemediationAutomation-ExecutionRolePolicy 1549
このポリシーを使用すると 1549
ポリシーの詳細 1549
ポリシーのバージョン 1549
JSON ポリシードキュメント 1549
詳細はこちら 1556
AWS-SSM-RemediationAutomation-OperationalAccountAdministrationRolePolicy 1556
このポリシーを使用すると 1556
ポリシーの詳細 1556
ポリシーのバージョン 1556
JSON ポリシードキュメント 1557
詳細はこちら 1557
AWS_ConfigRole 1558
このポリシーを使用すると 1558
ポリシーの詳細 1558
ポリシーのバージョン 1558
JSON ポリシードキュメント 1558
詳細はこちら 1601

AWSAccountActivityAccess 1601
このポリシーを使用すると 1602
ポリシーの詳細 1602
ポリシーのバージョン 1602
JSON ポリシードキュメント 1602
詳細はこちら 1603
AWSAccountManagementFullAccess 1603
このポリシーを使用すると 1603
ポリシーの詳細 1603
ポリシーのバージョン 1603
JSON ポリシードキュメント 1604
詳細はこちら 1604
AWSAccountManagementReadOnlyAccess 1604
このポリシーを使用すると 1604
ポリシーの詳細 1604
ポリシーのバージョン 1605
JSON ポリシードキュメント 1605
詳細はこちら 1605
AWSAccountSettingsManagementRole 1605
このポリシーを使用すると 1606
ポリシーの詳細 1606
ポリシーのバージョン 1606
JSON ポリシードキュメント 1606
詳細はこちら 1608
AWSAccountUsageReportAccess 1609
このポリシーを使用すると 1609
ポリシーの詳細 1609
ポリシーのバージョン 1609
JSON ポリシードキュメント 1609
詳細はこちら 1610
AWSAgentlessDiscoveryService 1610
このポリシーを使用すると 1610
ポリシーの詳細 1610
ポリシーのバージョン 1610
JSON ポリシードキュメント 1611
詳細はこちら 1612

AWSAppFabricFullAccess 1613
このポリシーを使用すると 1613
ポリシーの詳細 1613
ポリシーのバージョン 1613
JSON ポリシードキュメント 1613
詳細はこちら 1615
AWSAppFabricReadOnlyAccess 1615
このポリシーを使用すると 1615
ポリシーの詳細 1615
ポリシーのバージョン 1615
JSON ポリシードキュメント 1615
詳細はこちら 1616
AWSAppFabricServiceRolePolicy 1616
このポリシーを使用すると 1616
ポリシーの詳細 1616
ポリシーのバージョン 1617
JSON ポリシードキュメント 1617
詳細はこちら 1618
AWSApplicationAutoscalingAppStreamFleetPolicy 1618
このポリシーを使用すると 1618
ポリシーの詳細 1618
ポリシーのバージョン 1619
JSON ポリシードキュメント 1619
詳細はこちら 1619
AWSApplicationAutoscalingCassandraTablePolicy 1620
このポリシーを使用すると 1620
ポリシーの詳細 1620
ポリシーのバージョン 1620
JSON ポリシードキュメント 1620
詳細はこちら 1621
AWSApplicationAutoscalingComprehendEndpointPolicy 1621
このポリシーを使用すると 1621
ポリシーの詳細 1621
ポリシーのバージョン 1622
JSON ポリシードキュメント 1622
詳細はこちら 1622

AWSApplicationAutoScalingCustomResourcePolicy 1623
このポリシーを使用すると 1623
ポリシーの詳細 1623
ポリシーのバージョン 1623
JSON ポリシードキュメント 1623
詳細はこちら 1624
AWSApplicationAutoscalingDynamoDBTablePolicy 1624
このポリシーを使用すると 1624
ポリシーの詳細 1624
ポリシーのバージョン 1625
JSON ポリシードキュメント 1625
詳細はこちら 1625
AWSApplicationAutoscalingEC2SpotFleetRequestPolicy 1625
このポリシーを使用すると 1626
ポリシーの詳細 1626
ポリシーのバージョン 1626
JSON ポリシードキュメント 1626
詳細はこちら 1627
AWSApplicationAutoscalingECSServicePolicy 1627
このポリシーを使用すると 1627
ポリシーの詳細 1627
ポリシーのバージョン 1627
JSON ポリシードキュメント 1628
詳細はこちら 1628
AWSApplicationAutoscalingElastiCacheRGPolicy 1628
このポリシーを使用すると 1628
ポリシーの詳細 1629
ポリシーのバージョン 1629
JSON ポリシードキュメント 1629
詳細はこちら 1630
AWSApplicationAutoscalingEMRInstanceGroupPolicy 1630
このポリシーを使用すると 1630
ポリシーの詳細 1631
ポリシーのバージョン 1631
JSON ポリシードキュメント 1631
詳細はこちら 1631

AWSApplicationAutoscalingKafkaClusterPolicy 1632
このポリシーを使用すると 1632
ポリシーの詳細 1632
ポリシーのバージョン 1632
JSON ポリシードキュメント 1632
詳細はこちら 1633
AWSApplicationAutoscalingLambdaConcurrencyPolicy 1633
このポリシーを使用すると 1633
ポリシーの詳細 1633
ポリシーのバージョン 1634
JSON ポリシードキュメント 1634
詳細はこちら 1634
AWSApplicationAutoscalingNeptuneClusterPolicy 1634
このポリシーを使用すると 1635
ポリシーの詳細 1635
ポリシーのバージョン 1635
JSON ポリシードキュメント 1635
詳細はこちら 1637
AWSApplicationAutoscalingRDSClusterPolicy 1637
このポリシーを使用すると 1637
ポリシーの詳細 1637
ポリシーのバージョン 1637
JSON ポリシードキュメント 1638
詳細はこちら 1638
AWSApplicationAutoscalingSageMakerEndpointPolicy 1639
このポリシーを使用すると 1639
ポリシーの詳細 1639
ポリシーのバージョン 1639
JSON ポリシードキュメント 1639
詳細はこちら 1640
AWSApplicationAutoscalingWorkSpacesPoolPolicy 1640
このポリシーを使用すると 1641
ポリシーの詳細 1641
ポリシーのバージョン 1641
JSON ポリシードキュメント 1641
詳細はこちら 1642

AWSApplicationDiscoveryAgentAccess 1643
このポリシーを使用すると 1643
ポリシーの詳細 1643
ポリシーのバージョン 1643
JSON ポリシードキュメント 1643
詳細はこちら 1644
AWSApplicationDiscoveryAgentlessCollectorAccess 1644
このポリシーを使用すると 1644
ポリシーの詳細 1644
ポリシーのバージョン 1645
JSON ポリシードキュメント 1645
詳細はこちら 1646
AWSApplicationDiscoveryServiceFullAccess 1646
このポリシーを使用すると 1646
ポリシーの詳細 1646
ポリシーのバージョン 1646
JSON ポリシードキュメント 1647
詳細はこちら 1648
AWSApplicationMigrationAgentInstallationPolicy 1648
このポリシーを使用すると 1649
ポリシーの詳細 1649
ポリシーのバージョン 1649
JSON ポリシードキュメント 1649
詳細はこちら 1650
AWSApplicationMigrationAgentPolicy 1650
このポリシーを使用すると 1650
ポリシーの詳細 1651
ポリシーのバージョン 1651
JSON ポリシードキュメント 1651
詳細はこちら 1652
AWSApplicationMigrationAgentPolicy_v2 1652
このポリシーを使用すると 1652
ポリシーの詳細 1652
ポリシーのバージョン 1653
JSON ポリシードキュメント 1653
詳細はこちら 1653

AWSApplicationMigrationConversionServerPolicy 1654
このポリシーを使用すると 1654
ポリシーの詳細 1654
ポリシーのバージョン 1654
JSON ポリシードキュメント 1655
詳細はこちら 1655
AWSApplicationMigrationEC2Access 1655
このポリシーを使用すると 1655
ポリシーの詳細 1656
ポリシーのバージョン 1656
JSON ポリシードキュメント 1656
詳細はこちら 1664
AWSApplicationMigrationFullAccess 1664
このポリシーを使用すると 1664
ポリシーの詳細 1665
ポリシーのバージョン 1665
JSON ポリシードキュメント 1665
詳細はこちら 1671
AWSApplicationMigrationMGHAccess 1671
このポリシーを使用すると 1671
ポリシーの詳細 1672
ポリシーのバージョン 1672
JSON ポリシードキュメント 1672
詳細はこちら 1673
AWSApplicationMigrationNetworkMigrationCustomResource 1673
このポリシーを使用すると 1673
ポリシーの詳細 1673
ポリシーのバージョン 1673
JSON ポリシードキュメント 1674
詳細はこちら 1674
AWSApplicationMigrationNetworkMigrationMultiAccount 1674
このポリシーを使用すると 1675
ポリシーの詳細 1675
ポリシーのバージョン 1675
JSON ポリシードキュメント 1675
詳細はこちら 1699

AWSApplicationMigrationReadOnlyAccess 1700
このポリシーを使用すると 1700
ポリシーの詳細 1700
ポリシーのバージョン 1700
JSON ポリシードキュメント 1700
詳細はこちら 1701
AWSApplicationMigrationReplicationServerPolicy 1702
このポリシーを使用すると 1702
ポリシーの詳細 1702
ポリシーのバージョン 1702
JSON ポリシードキュメント 1703
詳細はこちら 1704
AWSApplicationMigrationServiceEc2InstancePolicy 1704
このポリシーを使用すると 1705
ポリシーの詳細 1705
ポリシーのバージョン 1705
JSON ポリシードキュメント 1705
詳細はこちら 1706
AWSApplicationMigrationServiceRolePolicy 1706
このポリシーを使用すると 1707
ポリシーの詳細 1707
ポリシーのバージョン 1707
JSON ポリシードキュメント 1707
詳細はこちら 1715
AWSApplicationMigrationSSMAccess 1715
このポリシーを使用すると 1715
ポリシーの詳細 1715
ポリシーのバージョン 1715
JSON ポリシードキュメント 1715
詳細はこちら 1717
AWSApplicationMigrationVCenterClientPolicy 1718
このポリシーを使用すると 1718
ポリシーの詳細 1718
ポリシーのバージョン 1718
JSON ポリシードキュメント 1718
詳細はこちら 1719

AWSAppMeshEnvoyAccess 1719
このポリシーを使用すると 1719
ポリシーの詳細 1719
ポリシーのバージョン 1720
JSON ポリシードキュメント 1720
詳細はこちら 1720
AWSAppMeshFullAccess 1720
このポリシーを使用すると 1721
ポリシーの詳細 1721
ポリシーのバージョン 1721
JSON ポリシードキュメント 1721
詳細はこちら 1722
AWSAppMeshPreviewEnvoyAccess 1723
このポリシーを使用すると 1723
ポリシーの詳細 1723
ポリシーのバージョン 1723
JSON ポリシードキュメント 1723
詳細はこちら 1724
AWSAppMeshPreviewServiceRolePolicy 1724
このポリシーを使用すると 1724
ポリシーの詳細 1724
ポリシーのバージョン 1724
JSON ポリシードキュメント 1725
詳細はこちら 1725
AWSAppMeshReadOnly 1725
このポリシーを使用すると 1726
ポリシーの詳細 1726
ポリシーのバージョン 1726
JSON ポリシードキュメント 1726
詳細はこちら 1727
AWSAppMeshServiceRolePolicy 1727
このポリシーを使用すると 1727
ポリシーの詳細 1728
ポリシーのバージョン 1728
JSON ポリシードキュメント 1728
詳細はこちら 1729

AWSAppRunnerFullAccess 1729
このポリシーを使用すると 1729
ポリシーの詳細 1729
ポリシーのバージョン 1729
JSON ポリシードキュメント 1729
詳細はこちら 1730
AWSAppRunnerReadOnlyAccess 1730
このポリシーを使用すると 1731
ポリシーの詳細 1731
ポリシーのバージョン 1731
JSON ポリシードキュメント 1731
詳細はこちら 1731
AWSAppRunnerServicePolicyForECRAccess 1732
このポリシーを使用すると 1732
ポリシーの詳細 1732
ポリシーのバージョン 1732
JSON ポリシードキュメント 1732
詳細はこちら 1733
AWSAppSyncAdministrator 1733
このポリシーを使用すると 1733
ポリシーの詳細 1733
ポリシーのバージョン 1734
JSON ポリシードキュメント 1734
詳細はこちら 1735
AWSAppSyncInvokeFullAccess 1735
このポリシーを使用すると 1735
ポリシーの詳細 1735
ポリシーのバージョン 1736
JSON ポリシードキュメント 1736
詳細はこちら 1736
AWSAppSyncPushToCloudWatchLogs 1736
このポリシーを使用すると 1737
ポリシーの詳細 1737
ポリシーのバージョン 1737
JSON ポリシードキュメント 1737
詳細はこちら 1737

AWSAppSyncSchemaAuthor 1738
このポリシーを使用すると 1738
ポリシーの詳細 1738
ポリシーのバージョン 1738
JSON ポリシードキュメント 1738
詳細はこちら 1739
AWSAppSyncServiceRolePolicy 1740
このポリシーを使用すると 1740
ポリシーの詳細 1740
ポリシーのバージョン 1740
JSON ポリシードキュメント 1740
詳細はこちら 1741
AWSArtifactAccountSync 1741
このポリシーを使用すると 1741
ポリシーの詳細 1741
ポリシーのバージョン 1741
JSON ポリシードキュメント 1742
詳細はこちら 1742
AWSArtifactAgreementsFullAccess 1742
このポリシーを使用すると 1742
ポリシーの詳細 1743
ポリシーのバージョン 1743
JSON ポリシードキュメント 1743
詳細はこちら 1745
AWSArtifactAgreementsReadOnlyAccess 1745
このポリシーを使用すると 1745
ポリシーの詳細 1746
ポリシーのバージョン 1746
JSON ポリシードキュメント 1746
詳細はこちら 1747
AWSArtifactReportsReadOnlyAccess 1747
このポリシーを使用すると 1747
ポリシーの詳細 1747
ポリシーのバージョン 1748
JSON ポリシードキュメント 1748
詳細はこちら 1748

AWSArtifactServiceRolePolicy 1749
このポリシーを使用すると 1749
ポリシーの詳細 1749
ポリシーのバージョン 1749
JSON ポリシードキュメント 1749
詳細はこちら 1750
AWSAuditManagerAdministratorAccess 1750
このポリシーを使用すると 1750
ポリシーの詳細 1750
ポリシーのバージョン 1750
JSON ポリシードキュメント 1751
詳細はこちら 1755
AWSAuditManagerServiceRolePolicy 1755
このポリシーを使用すると 1755
ポリシーの詳細 1755
ポリシーのバージョン 1755
JSON ポリシードキュメント 1756
詳細はこちら 1762
AWSAutoScalingPlansEC2AutoScalingPolicy 1762
このポリシーを使用すると 1763
ポリシーの詳細 1763
ポリシーのバージョン 1763
JSON ポリシードキュメント 1763
詳細はこちら 1764
AWSBackupAuditAccess 1764
このポリシーを使用すると 1764
ポリシーの詳細 1764
ポリシーのバージョン 1764
JSON ポリシードキュメント 1765
詳細はこちら 1766
AWSBackupDataTransferAccess 1766
このポリシーを使用すると 1766
ポリシーの詳細 1766
ポリシーのバージョン 1767
JSON ポリシードキュメント 1767
詳細はこちら 1767

AWSBackupFullAccess 1768
このポリシーを使用すると 1768
ポリシーの詳細 1768
ポリシーのバージョン 1768
JSON ポリシードキュメント 1768
詳細はこちら 1780
AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync 1780
このポリシーを使用すると 1780
ポリシーの詳細 1780
ポリシーのバージョン 1781
JSON ポリシードキュメント 1781
詳細はこちら 1782
AWSBackupGuardDutyRolePolicyForScans 1782
このポリシーを使用すると 1782
ポリシーの詳細 1782
ポリシーのバージョン 1782
JSON ポリシードキュメント 1782
詳細はこちら 1786
AWSBackupOperatorAccess 1787
このポリシーを使用すると 1787
ポリシーの詳細 1787
ポリシーのバージョン 1787
JSON ポリシードキュメント 1787
詳細はこちら 1796
AWSBackupOrganizationAdminAccess 1797
このポリシーを使用すると 1797
ポリシーの詳細 1797
ポリシーのバージョン 1797
JSON ポリシードキュメント 1797
詳細はこちら 1799
AWSBackupRestoreAccessForSAPHANA 1799
このポリシーを使用すると 1800
ポリシーの詳細 1800
ポリシーのバージョン 1800
JSON ポリシードキュメント 1800
詳細はこちら 1801

AWSBackupSearchOperatorAccess 1801
このポリシーを使用すると 1801
ポリシーの詳細 1801
ポリシーのバージョン 1802
JSON ポリシードキュメント 1802
詳細はこちら 1803
AWSBackupServiceLinkedRolePolicyForBackup 1804
このポリシーを使用すると 1804
ポリシーの詳細 1804
ポリシーのバージョン 1804
JSON ポリシードキュメント 1804
詳細はこちら 1815
AWSBackupServiceLinkedRolePolicyForBackupTest 1815
このポリシーを使用すると 1815
ポリシーの詳細 1815
ポリシーのバージョン 1815
JSON ポリシードキュメント 1815
詳細はこちら 1816
AWSBackupServiceRolePolicyForBackup 1816
このポリシーを使用すると 1816
ポリシーの詳細 1817
ポリシーのバージョン 1817
JSON ポリシードキュメント 1817
詳細はこちら 1831
AWSBackupServiceRolePolicyForIndexing 1831
このポリシーを使用すると 1832
ポリシーの詳細 1832
ポリシーのバージョン 1832
JSON ポリシードキュメント 1832
詳細はこちら 1833
AWSBackupServiceRolePolicyForItemRestores 1833
このポリシーを使用すると 1834
ポリシーの詳細 1834
ポリシーのバージョン 1834
JSON ポリシードキュメント 1834
詳細はこちら 1836

AWSBackupServiceRolePolicyForRestores 1836
このポリシーを使用すると 1836
ポリシーの詳細 1836
ポリシーのバージョン 1837
JSON ポリシードキュメント 1837
詳細はこちら 1851
AWSBackupServiceRolePolicyForS3Backup 1851
このポリシーを使用すると 1851
ポリシーの詳細 1851
ポリシーのバージョン 1851
JSON ポリシードキュメント 1852
詳細はこちら 1854
AWSBackupServiceRolePolicyForS3Restore 1854
このポリシーを使用すると 1854
ポリシーの詳細 1854
ポリシーのバージョン 1855
JSON ポリシードキュメント 1855
詳細はこちら 1856
AWSBackupServiceRolePolicyForScans 1856
このポリシーを使用すると 1857
ポリシーの詳細 1857
ポリシーのバージョン 1857
JSON ポリシードキュメント 1857
詳細はこちら 1858
AWSBatchFullAccess 1858
このポリシーを使用すると 1858
ポリシーの詳細 1858
ポリシーのバージョン 1859
JSON ポリシードキュメント 1859
詳細はこちら 1860
AWSBatchServiceEventTargetRole 1860
このポリシーを使用すると 1861
ポリシーの詳細 1861
ポリシーのバージョン 1861
JSON ポリシードキュメント 1861
詳細はこちら 1861

AWSBatchServiceRole 1862
このポリシーを使用すると 1862
ポリシーの詳細 1862
ポリシーのバージョン 1862
JSON ポリシードキュメント 1862
詳細はこちら 1865
AWSBatchServiceRolePolicyForSageMaker 1866
このポリシーを使用すると 1866
ポリシーの詳細 1866
ポリシーのバージョン 1866
JSON ポリシードキュメント 1866
詳細はこちら 1868
AWSBCMDataExportsServiceRolePolicy 1868
このポリシーを使用すると 1868
ポリシーの詳細 1868
ポリシーのバージョン 1868
JSON ポリシードキュメント 1869
詳細はこちら 1869
AWSBillingConductorFullAccess 1869
このポリシーを使用すると 1869
ポリシーの詳細 1870
ポリシーのバージョン 1870
JSON ポリシードキュメント 1870
詳細はこちら 1871
AWSBillingConductorReadOnlyAccess 1871
このポリシーを使用すると 1871
ポリシーの詳細 1871
ポリシーのバージョン 1871
JSON ポリシードキュメント 1872
詳細はこちら 1872
AWSBillingReadOnlyAccess 1872
このポリシーを使用すると 1872
ポリシーの詳細 1873
ポリシーのバージョン 1873
JSON ポリシードキュメント 1873
詳細はこちら 1875

AWSBillingServiceRolePolicy 1875
このポリシーを使用すると 1875
ポリシーの詳細 1876
ポリシーのバージョン 1876
JSON ポリシードキュメント 1876
詳細はこちら 1876
AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM 1877
このポリシーを使用すると 1877
ポリシーの詳細 1877
ポリシーのバージョン 1877
JSON ポリシードキュメント 1877
詳細はこちら 1878
AWSBudgetsActionsWithAWSResourceControlAccess 1879
このポリシーを使用すると 1879
ポリシーの詳細 1879
ポリシーのバージョン 1879
JSON ポリシードキュメント 1879
詳細はこちら 1881
AWSBudgetsReadOnlyAccess 1881
このポリシーを使用すると 1881
ポリシーの詳細 1881
ポリシーのバージョン 1881
JSON ポリシードキュメント 1881
詳細はこちら 1882
AWSBugBustFullAccess 1882
このポリシーを使用すると 1882
ポリシーの詳細 1882
ポリシーのバージョン 1883
JSON ポリシードキュメント 1883
詳細はこちら 1884
AWSBugBustPlayerAccess 1884
このポリシーを使用すると 1884
ポリシーの詳細 1884
ポリシーのバージョン 1885
JSON ポリシードキュメント 1885
詳細はこちら 1886

AWSBugBustServiceRolePolicy 1886
このポリシーを使用すると 1886
ポリシーの詳細 1886
ポリシーのバージョン 1886
JSON ポリシードキュメント 1887
詳細はこちら 1887
AWSCertificateManagerFullAccess 1887
このポリシーを使用すると 1888
ポリシーの詳細 1888
ポリシーのバージョン 1888
JSON ポリシードキュメント 1888
詳細はこちら 1889
AWSCertificateManagerPrivateCAAuditor 1889
このポリシーを使用すると 1889
ポリシーの詳細 1889
ポリシーのバージョン 1890
JSON ポリシードキュメント 1890
詳細はこちら 1891
AWSCertificateManagerPrivateCAFullAccess 1891
このポリシーを使用すると 1891
ポリシーの詳細 1891
ポリシーのバージョン 1891
JSON ポリシードキュメント 1891
詳細はこちら 1892
AWSCertificateManagerPrivateCAPrivilegedUser 1892
このポリシーを使用すると 1892
ポリシーの詳細 1892
ポリシーのバージョン 1893
JSON ポリシードキュメント 1893
詳細はこちら 1894
AWSCertificateManagerPrivateCAReadOnly 1894
このポリシーを使用すると 1894
ポリシーの詳細 1894
ポリシーのバージョン 1895
JSON ポリシードキュメント 1895
詳細はこちら 1895

AWSCertificateManagerPrivateCAUser 1896
このポリシーを使用すると 1896
ポリシーの詳細 1896
ポリシーのバージョン 1896
JSON ポリシードキュメント 1896
詳細はこちら 1897
AWSCertificateManagerReadOnly 1898
このポリシーを使用すると 1898
ポリシーの詳細 1898
ポリシーのバージョン 1898
JSON ポリシードキュメント 1898
詳細はこちら 1899
AWSChatbotServiceLinkedRolePolicy 1899
このポリシーを使用すると 1899
ポリシーの詳細 1899
ポリシーのバージョン 1899
JSON ポリシードキュメント 1900
詳細はこちら 1900
AWSCleanRoomsFullAccess 1901
このポリシーを使用すると 1901
ポリシーの詳細 1901
ポリシーのバージョン 1901
JSON ポリシードキュメント 1901
詳細はこちら 1906
AWSCleanRoomsFullAccessNoQuerying 1906
このポリシーを使用すると 1906
ポリシーの詳細 1906
ポリシーのバージョン 1906
JSON ポリシードキュメント 1907
詳細はこちら 1911
AWSCleanRoomsMLFullAccess 1912
このポリシーを使用すると 1912
ポリシーの詳細 1912
ポリシーのバージョン 1912
JSON ポリシードキュメント 1912
詳細はこちら 1916

AWSCleanRoomsMLReadOnlyAccess 1916
このポリシーを使用すると 1917
ポリシーの詳細 1917
ポリシーのバージョン 1917
JSON ポリシードキュメント 1917
詳細はこちら 1918
AWSCleanRoomsReadOnlyAccess 1918
このポリシーを使用すると 1919
ポリシーの詳細 1919
ポリシーのバージョン 1919
JSON ポリシードキュメント 1919
詳細はこちら 1920
AWSCleanRoomsServiceRolePolicy 1921
このポリシーを使用すると 1921
ポリシーの詳細 1921
ポリシーのバージョン 1921
JSON ポリシードキュメント 1921
詳細はこちら 1922
AWSCloud9Administrator 1922
このポリシーを使用すると 1922
ポリシーの詳細 1922
ポリシーのバージョン 1922
JSON ポリシードキュメント 1923
詳細はこちら 1924
AWSCloud9EnvironmentMember 1924
このポリシーを使用すると 1925
ポリシーの詳細 1925
ポリシーのバージョン 1925
JSON ポリシードキュメント 1925
詳細はこちら 1927
AWSCloud9ServiceRolePolicy 1927
このポリシーを使用すると 1927
ポリシーの詳細 1927
ポリシーのバージョン 1927
JSON ポリシードキュメント 1928
詳細はこちら 1930

AWSCloud9SSMInstanceProfile 1930
このポリシーを使用すると 1930
ポリシーの詳細 1930
ポリシーのバージョン 1931
JSON ポリシードキュメント 1931
詳細はこちら 1931
AWSCloud9User 1931
このポリシーを使用すると 1932
ポリシーの詳細 1932
ポリシーのバージョン 1932
JSON ポリシードキュメント 1932
詳細はこちら 1935
AWSCloudFormationFullAccess 1935
このポリシーを使用すると 1935
ポリシーの詳細 1935
ポリシーのバージョン 1935
JSON ポリシードキュメント 1935
詳細はこちら 1936
AWSCloudFormationReadOnlyAccess 1936
このポリシーを使用すると 1936
ポリシーの詳細 1936
ポリシーのバージョン 1936
JSON ポリシードキュメント 1937
詳細はこちら 1937
AWSCloudFrontLogger 1937
このポリシーを使用すると 1938
ポリシーの詳細 1938
ポリシーのバージョン 1938
JSON ポリシードキュメント 1938
詳細はこちら 1939
AWSCloudFrontVPCOriginServiceRolePolicy 1939
このポリシーを使用すると 1939
ポリシーの詳細 1939
ポリシーのバージョン 1939
JSON ポリシードキュメント 1939
詳細はこちら 1942

AWSCloudHSMFullAccess 1942
このポリシーを使用すると 1942
ポリシーの詳細 1943
ポリシーのバージョン 1943
JSON ポリシードキュメント 1943
詳細はこちら 1943
AWSCloudHSMReadOnlyAccess 1944
このポリシーを使用すると 1944
ポリシーの詳細 1944
ポリシーのバージョン 1944
JSON ポリシードキュメント 1944
詳細はこちら 1945
AWSCloudHSMRole 1945
このポリシーを使用すると 1945
ポリシーの詳細 1945
ポリシーのバージョン 1945
JSON ポリシードキュメント 1945
詳細はこちら 1946
AWSCloudMapDiscoverInstanceAccess 1946
このポリシーを使用すると 1946
ポリシーの詳細 1947
ポリシーのバージョン 1947
JSON ポリシードキュメント 1947
詳細はこちら 1947
AWSCloudMapFullAccess 1948
このポリシーを使用すると 1948
ポリシーの詳細 1948
ポリシーのバージョン 1948
JSON ポリシードキュメント 1948
詳細はこちら 1949
AWSCloudMapReadOnlyAccess 1949
このポリシーを使用すると 1949
ポリシーの詳細 1949
ポリシーのバージョン 1950
JSON ポリシードキュメント 1950
詳細はこちら 1950

AWSCloudMapRegisterInstanceAccess 1951
このポリシーを使用すると 1951
ポリシーの詳細 1951
ポリシーのバージョン 1951
JSON ポリシードキュメント 1951
詳細はこちら 1952
AWSCloudShellFullAccess 1952
このポリシーを使用すると 1952
ポリシーの詳細 1952
ポリシーのバージョン 1953
JSON ポリシードキュメント 1953
詳細はこちら 1953
AWSCloudTrail_FullAccess 1953
このポリシーを使用すると 1953
ポリシーの詳細 1954
ポリシーのバージョン 1954
JSON ポリシードキュメント 1954
詳細はこちら 1956
AWSCloudTrail_ReadOnlyAccess 1957
このポリシーを使用すると 1957
ポリシーの詳細 1957
ポリシーのバージョン 1957
JSON ポリシードキュメント 1957
詳細はこちら 1958
AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy 1958
このポリシーを使用すると 1958
ポリシーの詳細 1958
ポリシーのバージョン 1959
JSON ポリシードキュメント 1959
詳細はこちら 1959
AWSCodeArtifactAdminAccess 1959
このポリシーを使用すると 1959
ポリシーの詳細 1960
ポリシーのバージョン 1960
JSON ポリシードキュメント 1960
詳細はこちら 1961

AWSCodeArtifactReadOnlyAccess 1961
このポリシーを使用すると 1961
ポリシーの詳細 1961
ポリシーのバージョン 1961
JSON ポリシードキュメント 1961
詳細はこちら 1962
AWSCodeBuildAdminAccess 1962
このポリシーを使用すると 1963
ポリシーの詳細 1963
ポリシーのバージョン 1963
JSON ポリシードキュメント 1963
詳細はこちら 1966
AWSCodeBuildDeveloperAccess 1967
このポリシーを使用すると 1967
ポリシーの詳細 1967
ポリシーのバージョン 1967
JSON ポリシードキュメント 1967
詳細はこちら 1970
AWSCodeBuildReadOnlyAccess 1970
このポリシーを使用すると 1970
ポリシーの詳細 1970
ポリシーのバージョン 1971
JSON ポリシードキュメント 1971
詳細はこちら 1972
AWSCodeCommitFullAccess 1972
このポリシーを使用すると 1973
ポリシーの詳細 1973
ポリシーのバージョン 1973
JSON ポリシードキュメント 1973
詳細はこちら 1978
AWSCodeCommitPowerUser 1978
このポリシーを使用すると 1978
ポリシーの詳細 1978
ポリシーのバージョン 1978
JSON ポリシードキュメント 1979
詳細はこちら 1983

AWSCodeCommitReadOnly 1984
このポリシーを使用すると 1984
ポリシーの詳細 1984
ポリシーのバージョン 1984
JSON ポリシードキュメント 1984
詳細はこちら 1987
AWSCodeDeployDeployerAccess 1987
このポリシーを使用すると 1987
ポリシーの詳細 1987
ポリシーのバージョン 1987
JSON ポリシードキュメント 1988
詳細はこちら 1989
AWSCodeDeployFullAccess 1989
このポリシーを使用すると 1989
ポリシーの詳細 1990
ポリシーのバージョン 1990
JSON ポリシードキュメント 1990
詳細はこちら 1992
AWSCodeDeployReadOnlyAccess 1992
このポリシーを使用すると 1992
ポリシーの詳細 1992
ポリシーのバージョン 1992
JSON ポリシードキュメント 1992
詳細はこちら 1993
AWSCodeDeployRole 1994
このポリシーを使用すると 1994
ポリシーの詳細 1994
ポリシーのバージョン 1994
JSON ポリシードキュメント 1994
詳細はこちら 1995
AWSCodeDeployRoleForCloudFormation 1996
このポリシーを使用すると 1996
ポリシーの詳細 1996
ポリシーのバージョン 1996
JSON ポリシードキュメント 1996
詳細はこちら 1997

AWSCodeDeployRoleForECS 1997
このポリシーを使用すると 1997
ポリシーの詳細 1997
ポリシーのバージョン 1998
JSON ポリシードキュメント 1998
詳細はこちら 1999
AWSCodeDeployRoleForECSLimited 1999
このポリシーを使用すると 1999
ポリシーの詳細 1999
ポリシーのバージョン 1999
JSON ポリシードキュメント 2000
詳細はこちら 2001
AWSCodeDeployRoleForLambda 2002
このポリシーを使用すると 2002
ポリシーの詳細 2002
ポリシーのバージョン 2002
JSON ポリシードキュメント 2002
詳細はこちら 2003
AWSCodeDeployRoleForLambdaLimited 2004
このポリシーを使用すると 2004
ポリシーの詳細 2004
ポリシーのバージョン 2004
JSON ポリシードキュメント 2004
詳細はこちら 2005
AWSCodePipeline_FullAccess 2006
このポリシーを使用すると 2006
ポリシーの詳細 2006
ポリシーのバージョン 2006
JSON ポリシードキュメント 2006
詳細はこちら 2010
AWSCodePipeline_ReadOnlyAccess 2010
このポリシーを使用すると 2010
ポリシーの詳細 2010
ポリシーのバージョン 2011
JSON ポリシードキュメント 2011
詳細はこちら 2012

AWSCodePipelineApproverAccess 2012
このポリシーを使用すると 2012
ポリシーの詳細 2012
ポリシーのバージョン 2013
JSON ポリシードキュメント 2013
詳細はこちら 2013
AWSCodePipelineCustomActionAccess 2013
このポリシーを使用すると 2014
ポリシーの詳細 2014
ポリシーのバージョン 2014
JSON ポリシードキュメント 2014
詳細はこちら 2015
AWSCodeStarFullAccess 2015
このポリシーを使用すると 2015
ポリシーの詳細 2015
ポリシーのバージョン 2015
JSON ポリシードキュメント 2015
詳細はこちら 2016
AWSCodeStarNotificationsServiceRolePolicy 2016
このポリシーを使用すると 2017
ポリシーの詳細 2017
ポリシーのバージョン 2017
JSON ポリシードキュメント 2017
詳細はこちら 2018
AWSCodeStarServiceRole 2018
このポリシーを使用すると 2019
ポリシーの詳細 2019
ポリシーのバージョン 2019
JSON ポリシードキュメント 2019
詳細はこちら 2024
AWSCompromisedKeyQuarantine 2024
このポリシーを使用すると 2024
ポリシーの詳細 2024
ポリシーのバージョン 2025
JSON ポリシードキュメント 2025
詳細はこちら 2026

AWSCompromisedKeyQuarantineV2 2026
このポリシーを使用すると 2026
ポリシーの詳細 2026
ポリシーのバージョン 2026
JSON ポリシードキュメント 2027
詳細はこちら 2029
AWSCompromisedKeyQuarantineV3 2029
このポリシーを使用すると 2030
ポリシーの詳細 2030
ポリシーのバージョン 2030
JSON ポリシードキュメント 2030
詳細はこちら 2032
AWSConfigMultiAccountSetupPolicy 2033
このポリシーを使用すると 2033
ポリシーの詳細 2033
ポリシーのバージョン 2033
JSON ポリシードキュメント 2033
詳細はこちら 2035
AWSConfigRemediationServiceRolePolicy 2035
このポリシーを使用すると 2036
ポリシーの詳細 2036
ポリシーのバージョン 2036
JSON ポリシードキュメント 2036
詳細はこちら 2037
AWSConfigRoleForOrganizations 2037
このポリシーを使用すると 2037
ポリシーの詳細 2037
ポリシーのバージョン 2037
JSON ポリシードキュメント 2038
詳細はこちら 2038
AWSConfigRulesExecutionRole 2038
このポリシーを使用すると 2038
ポリシーの詳細 2039
ポリシーのバージョン 2039
JSON ポリシードキュメント 2039
詳細はこちら 2040

AWSConfigServiceRolePolicy 2040
このポリシーを使用すると 2040
ポリシーの詳細 2040
ポリシーのバージョン 2040
JSON ポリシードキュメント 2041
詳細はこちら 2084
AWSConfigUserAccess 2085
このポリシーを使用すると 2085
ポリシーの詳細 2085
ポリシーのバージョン 2085
JSON ポリシードキュメント 2085
詳細はこちら 2086
AWSConnector 2086
このポリシーを使用すると 2086
ポリシーの詳細 2086
ポリシーのバージョン 2087
JSON ポリシードキュメント 2087
詳細はこちら 2089
AWSControlTowerAccountServiceRolePolicy 2089
このポリシーを使用すると 2089
ポリシーの詳細 2089
ポリシーのバージョン 2089
JSON ポリシードキュメント 2090
詳細はこちら 2095
AWSControlTowerCloudTrailRolePolicy 2095
このポリシーを使用すると 2095
ポリシーの詳細 2095
ポリシーのバージョン 2095
JSON ポリシードキュメント 2096
詳細はこちら 2096
AWSControlTowerIdentityCenterManagementPolicy 2096
このポリシーを使用すると 2097
ポリシーの詳細 2097
ポリシーのバージョン 2097
JSON ポリシードキュメント 2097
詳細はこちら 2098

AWSControlTowerServiceRolePolicy 2098
このポリシーを使用すると 2099
ポリシーの詳細 2099
ポリシーのバージョン 2099
JSON ポリシードキュメント 2099
詳細はこちら 2104
AWSCostAndUsageReportAutomationPolicy 2104
このポリシーを使用すると 2104
ポリシーの詳細 2104
ポリシーのバージョン 2105
JSON ポリシードキュメント 2105
詳細はこちら 2106
AWSDataExchangeDataGrantOwnerFullAccess 2106
このポリシーを使用すると 2106
ポリシーの詳細 2106
ポリシーのバージョン 2107
JSON ポリシードキュメント 2107
詳細はこちら 2108
AWSDataExchangeDataGrantReceiverFullAccess 2108
このポリシーを使用すると 2109
ポリシーの詳細 2109
ポリシーのバージョン 2109
JSON ポリシードキュメント 2109
詳細はこちら 2111
AWSDataExchangeFullAccess 2111
このポリシーを使用すると 2111
ポリシーの詳細 2111
ポリシーのバージョン 2111
JSON ポリシードキュメント 2112
詳細はこちら 2115
AWSDataExchangeProviderFullAccess 2115
このポリシーを使用すると 2115
ポリシーの詳細 2116
ポリシーのバージョン 2116
JSON ポリシードキュメント 2116
詳細はこちら 2120

AWSDataExchangeReadOnly 2120
このポリシーを使用すると 2120
ポリシーの詳細 2120
ポリシーのバージョン 2120
JSON ポリシードキュメント 2121
詳細はこちら 2122
AWSDataExchangeServiceRolePolicyForLicenseManagement 2122
このポリシーを使用すると 2122
ポリシーの詳細 2122
ポリシーのバージョン 2123
JSON ポリシードキュメント 2123
詳細はこちら 2123
AWSDataExchangeServiceRolePolicyForOrganizationDiscovery 2124
このポリシーを使用すると 2124
ポリシーの詳細 2124
ポリシーのバージョン 2124
JSON ポリシードキュメント 2124
詳細はこちら 2125
AWSDataExchangeSubscriberFullAccess 2125
このポリシーを使用すると 2125
ポリシーの詳細 2125
ポリシーのバージョン 2126
JSON ポリシードキュメント 2126
詳細はこちら 2128
AWSDataLifecycleManagerServiceRole 2128
このポリシーを使用すると 2128
ポリシーの詳細 2128
ポリシーのバージョン 2129
JSON ポリシードキュメント 2129
詳細はこちら 2130
AWSDataLifecycleManagerServiceRoleForAMIManagement 2130
このポリシーを使用すると 2130
ポリシーの詳細 2131
ポリシーのバージョン 2131
JSON ポリシードキュメント 2131
詳細はこちら 2132

AWSDataLifecycleManagerSSMFullAccess 2132
このポリシーを使用すると 2133
ポリシーの詳細 2133
ポリシーのバージョン 2133
JSON ポリシードキュメント 2133
詳細はこちら 2134
AWSDataPipeline_FullAccess 2135
このポリシーを使用すると 2135
ポリシーの詳細 2135
ポリシーのバージョン 2135
JSON ポリシードキュメント 2135
詳細はこちら 2136
AWSDataPipeline_PowerUser 2136
このポリシーを使用すると 2137
ポリシーの詳細 2137
ポリシーのバージョン 2137
JSON ポリシードキュメント 2137
詳細はこちら 2138
AWSDataSyncDiscoveryServiceRolePolicy 2138
このポリシーを使用すると 2138
ポリシーの詳細 2138
ポリシーのバージョン 2139
JSON ポリシードキュメント 2139
詳細はこちら 2140
AWSDataSyncFullAccess 2140
このポリシーを使用すると 2140
ポリシーの詳細 2140
ポリシーのバージョン 2140
JSON ポリシードキュメント 2141
詳細はこちら 2143
AWSDataSyncReadOnlyAccess 2143
このポリシーを使用すると 2143
ポリシーの詳細 2144
ポリシーのバージョン 2144
JSON ポリシードキュメント 2144
詳細はこちら 2145

AWSDataSyncServiceRolePolicy 2145
このポリシーを使用すると 2145
ポリシーの詳細 2145
ポリシーのバージョン 2145
JSON ポリシードキュメント 2146
詳細はこちら 2147
AWSDeadlineCloud-FleetWorker 2147
このポリシーを使用すると 2147
ポリシーの詳細 2147
ポリシーのバージョン 2147
JSON ポリシードキュメント 2147
詳細はこちら 2148
AWSDeadlineCloud-UserAccessFarms 2148
このポリシーを使用すると 2148
ポリシーの詳細 2149
ポリシーのバージョン 2149
JSON ポリシードキュメント 2149
詳細はこちら 2154
AWSDeadlineCloud-UserAccessFleets 2155
このポリシーを使用すると 2155
ポリシーの詳細 2155
ポリシーのバージョン 2155
JSON ポリシードキュメント 2155
詳細はこちら 2159
AWSDeadlineCloud-UserAccessJobs 2159
このポリシーを使用すると 2159
ポリシーの詳細 2159
ポリシーのバージョン 2160
JSON ポリシードキュメント 2160
詳細はこちら 2164
AWSDeadlineCloud-UserAccessQueues 2164
このポリシーを使用すると 2164
ポリシーの詳細 2164
ポリシーのバージョン 2164
JSON ポリシードキュメント 2165
詳細はこちら 2169

AWSDeadlineCloud-WorkerHost 2169
このポリシーを使用すると 2170
ポリシーの詳細 2170
ポリシーのバージョン 2170
JSON ポリシードキュメント 2170
詳細はこちら 2171
AWSDeepLensLambdaFunctionAccessPolicy 2171
このポリシーを使用すると 2172
ポリシーの詳細 2172
ポリシーのバージョン 2172
JSON ポリシードキュメント 2172
詳細はこちら 2173
AWSDeepLensServiceRolePolicy 2174
このポリシーを使用すると 2174
ポリシーの詳細 2174
ポリシーのバージョン 2174
JSON ポリシードキュメント 2174
詳細はこちら 2181
AWSDeepRacerAccountAdminAccess 2182
このポリシーを使用すると 2182
ポリシーの詳細 2182
ポリシーのバージョン 2182
JSON ポリシードキュメント 2182
詳細はこちら 2183
AWSDeepRacerCloudFormationAccessPolicy 2183
このポリシーを使用すると 2183
ポリシーの詳細 2183
ポリシーのバージョン 2183
JSON ポリシードキュメント 2184
詳細はこちら 2187
AWSDeepRacerDefaultMultiUserAccess 2187
このポリシーを使用すると 2187
ポリシーの詳細 2187
ポリシーのバージョン 2187
JSON ポリシードキュメント 2187
詳細はこちら 2189

AWSDeepRacerFullAccess 2189
このポリシーを使用すると 2189
ポリシーの詳細 2189
ポリシーのバージョン 2190
JSON ポリシードキュメント 2190
詳細はこちら 2191
AWSDeepRacerRoboMakerAccessPolicy 2191
このポリシーを使用すると 2191
ポリシーの詳細 2191
ポリシーのバージョン 2191
JSON ポリシードキュメント 2192
詳細はこちら 2194
AWSDeepRacerServiceRolePolicy 2194
このポリシーを使用すると 2194
ポリシーの詳細 2194
ポリシーのバージョン 2194
JSON ポリシードキュメント 2194
詳細はこちら 2198
AWSDenyAll 2198
このポリシーを使用すると 2198
ポリシーの詳細 2198
ポリシーのバージョン 2198
JSON ポリシードキュメント 2198
詳細はこちら 2199
AWSDeviceFarmFullAccess 2199
このポリシーを使用すると 2199
ポリシーの詳細 2199
ポリシーのバージョン 2199
JSON ポリシードキュメント 2200
詳細はこちら 2200
AWSDeviceFarmServiceRolePolicy 2200
このポリシーを使用すると 2200
ポリシーの詳細 2201
ポリシーのバージョン 2201
JSON ポリシードキュメント 2201
詳細はこちら 2203

AWSDeviceFarmTestGridServiceRolePolicy 2203
このポリシーを使用すると 2203
ポリシーの詳細 2203
ポリシーのバージョン 2204
JSON ポリシードキュメント 2204
詳細はこちら 2206
AWSDirectConnectFullAccess 2206
このポリシーを使用すると 2206
ポリシーの詳細 2206
ポリシーのバージョン 2207
JSON ポリシードキュメント 2207
詳細はこちら 2207
AWSDirectConnectReadOnlyAccess 2207
このポリシーを使用すると 2208
ポリシーの詳細 2208
ポリシーのバージョン 2208
JSON ポリシードキュメント 2208
詳細はこちら 2209
AWSDirectConnectServiceRolePolicy 2209
このポリシーを使用すると 2209
ポリシーの詳細 2209
ポリシーのバージョン 2209
JSON ポリシードキュメント 2210
詳細はこちら 2210
AWSDirectoryServiceDataFullAccess 2210
このポリシーを使用すると 2210
ポリシーの詳細 2210
ポリシーのバージョン 2211
JSON ポリシードキュメント 2211
詳細はこちら 2212
AWSDirectoryServiceDataReadOnlyAccess 2212
このポリシーを使用すると 2212
ポリシーの詳細 2212
ポリシーのバージョン 2212
JSON ポリシードキュメント 2213
詳細はこちら 2213

AWSDirectoryServiceFullAccess 2213
このポリシーを使用すると 2214
ポリシーの詳細 2214
ポリシーのバージョン 2214
JSON ポリシードキュメント 2214
詳細はこちら 2216
AWSDirectoryServiceReadOnlyAccess 2216
このポリシーを使用すると 2216
ポリシーの詳細 2216
ポリシーのバージョン 2217
JSON ポリシードキュメント 2217
詳細はこちら 2217
AWSDirectoryServiceServiceRolePolicy 2218
このポリシーを使用すると 2218
ポリシーの詳細 2218
ポリシーのバージョン 2218
JSON ポリシードキュメント 2218
詳細はこちら 2219
AWSDiscoveryContinuousExportFirehosePolicy 2220
このポリシーを使用すると 2220
ポリシーの詳細 2220
ポリシーのバージョン 2220
JSON ポリシードキュメント 2220
詳細はこちら 2221
AWSDMSFleetAdvisorServiceRolePolicy 2221
このポリシーを使用すると 2222
ポリシーの詳細 2222
ポリシーのバージョン 2222
JSON ポリシードキュメント 2222
詳細はこちら 2223
AWSDMSServerlessServiceRolePolicy 2223
このポリシーを使用すると 2223
ポリシーの詳細 2223
ポリシーのバージョン 2223
JSON ポリシードキュメント 2223
詳細はこちら 2226

AWSEC2CapacityManagerServiceRolePolicy 2226
このポリシーを使用すると 2227
ポリシーの詳細 2227
ポリシーのバージョン 2227
JSON ポリシードキュメント 2227
詳細はこちら 2228
AWSEC2CapacityReservationFleetRolePolicy 2228
このポリシーを使用すると 2228
ポリシーの詳細 2228
ポリシーのバージョン 2229
JSON ポリシードキュメント 2229
詳細はこちら 2230
AWSEC2FleetServiceRolePolicy 2230
このポリシーを使用すると 2230
ポリシーの詳細 2230
ポリシーのバージョン 2231
JSON ポリシードキュメント 2231
詳細はこちら 2233
AWSEC2SpotFleetServiceRolePolicy 2233
このポリシーを使用すると 2233
ポリシーの詳細 2233
ポリシーのバージョン 2234
JSON ポリシードキュメント 2234
詳細はこちら 2236
AWSEC2SpotServiceRolePolicy 2236
このポリシーを使用すると 2236
ポリシーの詳細 2236
ポリシーのバージョン 2236
JSON ポリシードキュメント 2236
詳細はこちら 2238
AWSEC2SqlHaInstancePolicy 2238
このポリシーを使用すると 2238
ポリシーの詳細 2238
ポリシーのバージョン 2239
JSON ポリシードキュメント 2239
詳細はこちら 2240

AWSEC2SqlHaServiceRolePolicy 2240
このポリシーを使用すると 2240
ポリシーの詳細 2241
ポリシーのバージョン 2241
JSON ポリシードキュメント 2241
詳細はこちら 2243
AWSEC2VssSnapshotPolicy 2243
このポリシーを使用すると 2243
ポリシーの詳細 2243
ポリシーのバージョン 2243
JSON ポリシードキュメント 2244
詳細はこちら 2247
AWSECRPullThroughCache_ServiceRolePolicy 2247
このポリシーを使用すると 2247
ポリシーの詳細 2247
ポリシーのバージョン 2248
JSON ポリシードキュメント 2248
詳細はこちら 2249
AWSElasticBeanstalkCustomPlatformforEC2Role 2249
このポリシーを使用すると 2249
ポリシーの詳細 2249
ポリシーのバージョン 2249
JSON ポリシードキュメント 2250
詳細はこちら 2251
AWSElasticBeanstalkEnhancedHealth 2252
このポリシーを使用すると 2252
ポリシーの詳細 2252
ポリシーのバージョン 2252
JSON ポリシードキュメント 2252
詳細はこちら 2253
AWSElasticBeanstalkMaintenance 2253
このポリシーを使用すると 2254
ポリシーの詳細 2254
ポリシーのバージョン 2254
JSON ポリシードキュメント 2254
詳細はこちら 2255

AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy 2255
このポリシーを使用すると 2255
ポリシーの詳細 2256
ポリシーのバージョン 2256
JSON ポリシードキュメント 2256
詳細はこちら 2263
AWSElasticBeanstalkManagedUpdatesServiceRolePolicy 2263
このポリシーを使用すると 2263
ポリシーの詳細 2263
ポリシーのバージョン 2264
JSON ポリシードキュメント 2264
詳細はこちら 2269
AWSElasticBeanstalkMulticontainerDocker 2269
このポリシーを使用すると 2270
ポリシーの詳細 2270
ポリシーのバージョン 2270
JSON ポリシードキュメント 2270
詳細はこちら 2271
AWSElasticBeanstalkReadOnly 2271
このポリシーを使用すると 2271
ポリシーの詳細 2272
ポリシーのバージョン 2272
JSON ポリシードキュメント 2272
詳細はこちら 2274
AWSElasticBeanstalkRoleCore 2274
このポリシーを使用すると 2274
ポリシーの詳細 2275
ポリシーのバージョン 2275
JSON ポリシードキュメント 2275
詳細はこちら 2280
AWSElasticBeanstalkRoleCWL 2280
このポリシーを使用すると 2280
ポリシーの詳細 2280
ポリシーのバージョン 2281
JSON ポリシードキュメント 2281
詳細はこちら 2281

AWSElasticBeanstalkRoleECS 2281
このポリシーを使用すると 2282
ポリシーの詳細 2282
ポリシーのバージョン 2282
JSON ポリシードキュメント 2282
詳細はこちら 2283
AWSElasticBeanstalkRoleRDS 2283
このポリシーを使用すると 2283
ポリシーの詳細 2283
ポリシーのバージョン 2284
JSON ポリシードキュメント 2284
詳細はこちら 2284
AWSElasticBeanstalkRoleSNS 2285
このポリシーを使用すると 2285
ポリシーの詳細 2285
ポリシーのバージョン 2285
JSON ポリシードキュメント 2285
詳細はこちら 2286
AWSElasticBeanstalkRoleWorkerTier 2286
このポリシーを使用すると 2286
ポリシーの詳細 2287
ポリシーのバージョン 2287
JSON ポリシードキュメント 2287
詳細はこちら 2288
AWSElasticBeanstalkService 2288
このポリシーを使用すると 2288
ポリシーの詳細 2288
ポリシーのバージョン 2288
JSON ポリシードキュメント 2289
詳細はこちら 2293
AWSElasticBeanstalkServiceRolePolicy 2293
このポリシーを使用すると 2293
ポリシーの詳細 2293
ポリシーのバージョン 2294
JSON ポリシードキュメント 2294
詳細はこちら 2295

AWSElasticBeanstalkWebTier 2295
このポリシーを使用すると 2296
ポリシーの詳細 2296
ポリシーのバージョン 2296
JSON ポリシードキュメント 2296
詳細はこちら 2297
AWSElasticBeanstalkWorkerTier 2298
このポリシーを使用すると 2298
ポリシーの詳細 2298
ポリシーのバージョン 2298
JSON ポリシードキュメント 2298
詳細はこちら 2300
AWSElasticDisasterRecoveryAgentInstallationPolicy 2301
このポリシーを使用すると 2301
ポリシーの詳細 2301
ポリシーのバージョン 2301
JSON ポリシードキュメント 2302
詳細はこちら 2303
AWSElasticDisasterRecoveryAgentPolicy 2303
このポリシーを使用すると 2303
ポリシーの詳細 2304
ポリシーのバージョン 2304
JSON ポリシードキュメント 2304
詳細はこちら 2305
AWSElasticDisasterRecoveryConsoleFullAccess 2305
このポリシーを使用すると 2305
ポリシーの詳細 2305
ポリシーのバージョン 2306
JSON ポリシードキュメント 2306
詳細はこちら 2316
AWSElasticDisasterRecoveryConsoleFullAccess_v2 2316
このポリシーを使用すると 2316
ポリシーの詳細 2316
ポリシーのバージョン 2317
JSON ポリシードキュメント 2317
詳細はこちら 2332

AWSElasticDisasterRecoveryConversionServerPolicy 2332
このポリシーを使用すると 2333
ポリシーの詳細 2333
ポリシーのバージョン 2333
JSON ポリシードキュメント 2333
詳細はこちら 2334
AWSElasticDisasterRecoveryCrossAccountReplicationPolicy 2334
このポリシーを使用すると 2334
ポリシーの詳細 2334
ポリシーのバージョン 2335
JSON ポリシードキュメント 2335
詳細はこちら 2336
AWSElasticDisasterRecoveryEc2InstancePolicy 2336
このポリシーを使用すると 2336
ポリシーの詳細 2336
ポリシーのバージョン 2336
JSON ポリシードキュメント 2337
詳細はこちら 2339
AWSElasticDisasterRecoveryFailbackInstallationPolicy 2339
このポリシーを使用すると 2339
ポリシーの詳細 2339
ポリシーのバージョン 2339
JSON ポリシードキュメント 2340
詳細はこちら 2340
AWSElasticDisasterRecoveryFailbackPolicy 2341
このポリシーを使用すると 2341
ポリシーの詳細 2341
ポリシーのバージョン 2341
JSON ポリシードキュメント 2341
詳細はこちら 2343
AWSElasticDisasterRecoveryLaunchActionsPolicy 2343
このポリシーを使用すると 2343
ポリシーの詳細 2343
ポリシーのバージョン 2343
JSON ポリシードキュメント 2344
詳細はこちら 2350

AWSElasticDisasterRecoveryNetworkReplicationPolicy 2350
このポリシーを使用すると 2350
ポリシーの詳細 2350
ポリシーのバージョン 2350
JSON ポリシードキュメント 2351
詳細はこちら 2351
AWSElasticDisasterRecoveryReadOnlyAccess 2351
このポリシーを使用すると 2352
ポリシーの詳細 2352
ポリシーのバージョン 2352
JSON ポリシードキュメント 2352
詳細はこちら 2354
AWSElasticDisasterRecoveryRecoveryInstancePolicy 2355
このポリシーを使用すると 2355
ポリシーの詳細 2355
ポリシーのバージョン 2355
JSON ポリシードキュメント 2355
詳細はこちら 2358
AWSElasticDisasterRecoveryReplicationServerPolicy 2358
このポリシーを使用すると 2359
ポリシーの詳細 2359
ポリシーのバージョン 2359
JSON ポリシードキュメント 2359
詳細はこちら 2361
AWSElasticDisasterRecoveryServiceRolePolicy 2361
このポリシーを使用すると 2362
ポリシーの詳細 2362
ポリシーのバージョン 2362
JSON ポリシードキュメント 2362
詳細はこちら 2372
AWSElasticDisasterRecoveryStagingAccountPolicy 2372
このポリシーを使用すると 2372
ポリシーの詳細 2373
ポリシーのバージョン 2373
JSON ポリシードキュメント 2373
詳細はこちら 2374

AWSElasticDisasterRecoveryStagingAccountPolicy_v2 2374
このポリシーを使用すると 2374
ポリシーの詳細 2374
ポリシーのバージョン 2375
JSON ポリシードキュメント 2375
詳細はこちら 2376
AWSElasticLoadBalancingClassicServiceRolePolicy 2376
このポリシーを使用すると 2376
ポリシーの詳細 2376
ポリシーのバージョン 2377
JSON ポリシードキュメント 2377
詳細はこちら 2378
AWSElasticLoadBalancingServiceRolePolicy 2378
このポリシーを使用すると 2378
ポリシーの詳細 2378
ポリシーのバージョン 2378
JSON ポリシードキュメント 2379
詳細はこちら 2380
AWSElementalMediaConnectFullAccess 2380
このポリシーを使用すると 2380
ポリシーの詳細 2380
ポリシーのバージョン 2380
JSON ポリシードキュメント 2381
詳細はこちら 2381
AWSElementalMediaConnectReadOnlyAccess 2381
このポリシーを使用すると 2381
ポリシーの詳細 2382
ポリシーのバージョン 2382
JSON ポリシードキュメント 2382
詳細はこちら 2383
AWSElementalMediaConvertFullAccess 2383
このポリシーを使用すると 2383
ポリシーの詳細 2383
ポリシーのバージョン 2383
JSON ポリシードキュメント 2384
詳細はこちら 2384

AWSElementalMediaConvertReadOnly 2385
このポリシーを使用すると 2385
ポリシーの詳細 2385
ポリシーのバージョン 2385
JSON ポリシードキュメント 2385
詳細はこちら 2386
AWSElementalMediaLiveFullAccess 2386
このポリシーを使用すると 2386
ポリシーの詳細 2386
ポリシーのバージョン 2386
JSON ポリシードキュメント 2387
詳細はこちら 2387
AWSElementalMediaLiveReadOnly 2387
このポリシーを使用すると 2387
ポリシーの詳細 2387
ポリシーのバージョン 2388
JSON ポリシードキュメント 2388
詳細はこちら 2388
AWSElementalMediaPackageFullAccess 2388
このポリシーを使用すると 2389
ポリシーの詳細 2389
ポリシーのバージョン 2389
JSON ポリシードキュメント 2389
詳細はこちら 2389
AWSElementalMediaPackageReadOnly 2390
このポリシーを使用すると 2390
ポリシーの詳細 2390
ポリシーのバージョン 2390
JSON ポリシードキュメント 2390
詳細はこちら 2391
AWSElementalMediaPackageV2FullAccess 2391
このポリシーを使用すると 2391
ポリシーの詳細 2391
ポリシーのバージョン 2391
JSON ポリシードキュメント 2391
詳細はこちら 2392

AWSElementalMediaPackageV2ReadOnly 2392
このポリシーを使用すると 2392
ポリシーの詳細 2392
ポリシーのバージョン 2392
JSON ポリシードキュメント 2393
詳細はこちら 2393
AWSElementalMediaStoreFullAccess 2393
このポリシーを使用すると 2393
ポリシーの詳細 2393
ポリシーのバージョン 2394
JSON ポリシードキュメント 2394
詳細はこちら 2394
AWSElementalMediaStoreReadOnly 2395
このポリシーを使用すると 2395
ポリシーの詳細 2395
ポリシーのバージョン 2395
JSON ポリシードキュメント 2395
詳細はこちら 2396
AWSElementalMediaTailorFullAccess 2396
このポリシーを使用すると 2396
ポリシーの詳細 2396
ポリシーのバージョン 2396
JSON ポリシードキュメント 2397
詳細はこちら 2397
AWSElementalMediaTailorReadOnly 2397
このポリシーを使用すると 2397
ポリシーの詳細 2397
ポリシーのバージョン 2398
JSON ポリシードキュメント 2398
詳細はこちら 2398
AWSEnhancedClassicNetworkingMangementPolicy 2398
このポリシーを使用すると 2399
ポリシーの詳細 2399
ポリシーのバージョン 2399
JSON ポリシードキュメント 2399
詳細はこちら 2400

AWSEntityResolutionConsoleFullAccess 2400
このポリシーを使用すると 2400
ポリシーの詳細 2400
ポリシーのバージョン 2400
JSON ポリシードキュメント 2400
詳細はこちら 2404
AWSEntityResolutionConsoleReadOnlyAccess 2404
このポリシーを使用すると 2404
ポリシーの詳細 2404
ポリシーのバージョン 2404
JSON ポリシードキュメント 2404
詳細はこちら 2405
AWSFaultInjectionSimulatorEC2Access 2405
このポリシーを使用すると 2405
ポリシーの詳細 2405
ポリシーのバージョン 2406
JSON ポリシードキュメント 2406
詳細はこちら 2407
AWSFaultInjectionSimulatorECSAccess 2408
このポリシーを使用すると 2408
ポリシーの詳細 2408
ポリシーのバージョン 2408
JSON ポリシードキュメント 2408
詳細はこちら 2411
AWSFaultInjectionSimulatorEKSAccess 2411
このポリシーを使用すると 2411
ポリシーの詳細 2411
ポリシーのバージョン 2411
JSON ポリシードキュメント 2412
詳細はこちら 2413
AWSFaultInjectionSimulatorNetworkAccess 2413
このポリシーを使用すると 2413
ポリシーの詳細 2413
ポリシーのバージョン 2413
JSON ポリシードキュメント 2414
詳細はこちら 2420

AWSFaultInjectionSimulatorRDSAccess 2421
このポリシーを使用すると 2421
ポリシーの詳細 2421
ポリシーのバージョン 2421
JSON ポリシードキュメント 2421
詳細はこちら 2422
AWSFaultInjectionSimulatorSSMAccess 2423
このポリシーを使用すると 2423
ポリシーの詳細 2423
ポリシーのバージョン 2423
JSON ポリシードキュメント 2423
詳細はこちら 2425
AWSFinSpaceServiceRolePolicy 2425
このポリシーを使用すると 2425
ポリシーの詳細 2425
ポリシーのバージョン 2425
JSON ポリシードキュメント 2426
詳細はこちら 2426
AWSFMAdminFullAccess 2426
このポリシーを使用すると 2426
ポリシーの詳細 2427
ポリシーのバージョン 2427
JSON ポリシードキュメント 2427
詳細はこちら 2429
AWSFMAdminReadOnlyAccess 2429
このポリシーを使用すると 2429
ポリシーの詳細 2429
ポリシーのバージョン 2429
JSON ポリシードキュメント 2430
詳細はこちら 2431
AWSFMMemberReadOnlyAccess 2431
このポリシーを使用すると 2432
ポリシーの詳細 2432
ポリシーのバージョン 2432
JSON ポリシードキュメント 2432
詳細はこちら 2433

AWSForWordPressPluginPolicy 2433
このポリシーを使用すると 2433
ポリシーの詳細 2433
ポリシーのバージョン 2433
JSON ポリシードキュメント 2433
詳細はこちら 2435
AWSGitSyncServiceRolePolicy 2435
このポリシーを使用すると 2436
ポリシーの詳細 2436
ポリシーのバージョン 2436
JSON ポリシードキュメント 2436
詳細はこちら 2437
AWSGlobalAcceleratorSLRPolicy 2437
このポリシーを使用すると 2437
ポリシーの詳細 2437
ポリシーのバージョン 2437
JSON ポリシードキュメント 2438
詳細はこちら 2439
AWSGlueConsoleFullAccess 2439
このポリシーを使用すると 2440
ポリシーの詳細 2440
ポリシーのバージョン 2440
JSON ポリシードキュメント 2440
詳細はこちら 2444
AWSGlueConsoleSageMakerNotebookFullAccess 2444
このポリシーを使用すると 2445
ポリシーの詳細 2445
ポリシーのバージョン 2445
JSON ポリシードキュメント 2445
詳細はこちら 2450
AwsGlueDataBrewFullAccessPolicy 2450
このポリシーを使用すると 2451
ポリシーの詳細 2451
ポリシーのバージョン 2451
JSON ポリシードキュメント 2451
詳細はこちら 2456

AWSGlueDataBrewServiceRole 2456
このポリシーを使用すると 2457
ポリシーの詳細 2457
ポリシーのバージョン 2457
JSON ポリシードキュメント 2457
詳細はこちら 2460
AWSGlueSchemaRegistryFullAccess 2460
このポリシーを使用すると 2460
ポリシーの詳細 2460
ポリシーのバージョン 2461
JSON ポリシードキュメント 2461
詳細はこちら 2462
AWSGlueSchemaRegistryReadonlyAccess 2462
このポリシーを使用すると 2462
ポリシーの詳細 2462
ポリシーのバージョン 2463
JSON ポリシードキュメント 2463
詳細はこちら 2463
AWSGlueServiceNotebookRole 2464
このポリシーを使用すると 2464
ポリシーの詳細 2464
ポリシーのバージョン 2464
JSON ポリシードキュメント 2464
詳細はこちら 2467
AWSGlueServiceRole 2467
このポリシーを使用すると 2467
ポリシーの詳細 2467
ポリシーのバージョン 2467
JSON ポリシードキュメント 2467
詳細はこちら 2470
AwsGlueSessionUserRestrictedNotebookPolicy 2470
このポリシーを使用すると 2470
ポリシーの詳細 2470
ポリシーのバージョン 2470
JSON ポリシードキュメント 2471
詳細はこちら 2473

AwsGlueSessionUserRestrictedNotebookServiceRole 2474
このポリシーを使用すると 2474
ポリシーの詳細 2474
ポリシーのバージョン 2474
JSON ポリシードキュメント 2474
詳細はこちら 2478
AwsGlueSessionUserRestrictedPolicy 2478
このポリシーを使用すると 2479
ポリシーの詳細 2479
ポリシーのバージョン 2479
JSON ポリシードキュメント 2479
詳細はこちら 2482
AwsGlueSessionUserRestrictedServiceRole 2482
このポリシーを使用すると 2482
ポリシーの詳細 2482
ポリシーのバージョン 2483
JSON ポリシードキュメント 2483
詳細はこちら 2487
AWSGrafanaAccountAdministrator 2487
このポリシーを使用すると 2488
ポリシーの詳細 2488
ポリシーのバージョン 2488
JSON ポリシードキュメント 2488
詳細はこちら 2489
AWSGrafanaConsoleReadOnlyAccess 2489
このポリシーを使用すると 2489
ポリシーの詳細 2490
ポリシーのバージョン 2490
JSON ポリシードキュメント 2490
詳細はこちら 2490
AWSGrafanaWorkspacePermissionManagement 2491
このポリシーを使用すると 2491
ポリシーの詳細 2491
ポリシーのバージョン 2491
JSON ポリシードキュメント 2491
詳細はこちら 2492

AWSGrafanaWorkspacePermissionManagementV2 2492
このポリシーを使用すると 2493
ポリシーの詳細 2493
ポリシーのバージョン 2493
JSON ポリシードキュメント 2493
詳細はこちら 2494
AWSGreengrassFullAccess 2494
このポリシーを使用すると 2494
ポリシーの詳細 2494
ポリシーのバージョン 2495
JSON ポリシードキュメント 2495
詳細はこちら 2495
AWSGreengrassReadOnlyAccess 2495
このポリシーを使用すると 2496
ポリシーの詳細 2496
ポリシーのバージョン 2496
JSON ポリシードキュメント 2496
詳細はこちら 2496
AWSGreengrassResourceAccessRolePolicy 2497
このポリシーを使用すると 2497
ポリシーの詳細 2497
ポリシーのバージョン 2497
JSON ポリシードキュメント 2497
詳細はこちら 2500
AWSGroundStationAgentInstancePolicy 2500
このポリシーを使用すると 2500
ポリシーの詳細 2500
ポリシーのバージョン 2500
JSON ポリシードキュメント 2501
詳細はこちら 2501
AWSHealth_EventProcessorServiceRolePolicy 2501
このポリシーを使用すると 2501
ポリシーの詳細 2502
ポリシーのバージョン 2502
JSON ポリシードキュメント 2502
詳細はこちら 2503

AWSHealthFullAccess 2503
このポリシーを使用すると 2503
ポリシーの詳細 2503
ポリシーのバージョン 2503
JSON ポリシードキュメント 2504
詳細はこちら 2505
AWSHealthImagingFullAccess 2505
このポリシーを使用すると 2505
ポリシーの詳細 2505
ポリシーのバージョン 2505
JSON ポリシードキュメント 2505
詳細はこちら 2506
AWSHealthImagingReadOnlyAccess 2506
このポリシーを使用すると 2506
ポリシーの詳細 2506
ポリシーのバージョン 2507
JSON ポリシードキュメント 2507
詳細はこちら 2507
AWSIAMIdentityCenterAllowListForIdentityContext 2508
このポリシーを使用すると 2508
ポリシーの詳細 2508
ポリシーのバージョン 2508
JSON ポリシードキュメント 2508
詳細はこちら 2511
AWSIdentityCenterExternalManagementPolicy 2512
このポリシーを使用すると 2512
ポリシーの詳細 2512
ポリシーのバージョン 2512
JSON ポリシードキュメント 2512
詳細はこちら 2514
AWSIdentitySyncFullAccess 2514
このポリシーを使用すると 2514
ポリシーの詳細 2515
ポリシーのバージョン 2515
JSON ポリシードキュメント 2515
詳細はこちら 2516

AWSIdentitySyncReadOnlyAccess 2516
このポリシーを使用すると 2516
ポリシーの詳細 2516
ポリシーのバージョン 2516
JSON ポリシードキュメント 2517
詳細はこちら 2517
AWSImageBuilderFullAccess 2517
このポリシーを使用すると 2517
ポリシーの詳細 2518
ポリシーのバージョン 2518
JSON ポリシードキュメント 2518
詳細はこちら 2521
AWSImageBuilderReadOnlyAccess 2521
このポリシーを使用すると 2521
ポリシーの詳細 2521
ポリシーのバージョン 2521
JSON ポリシードキュメント 2521
詳細はこちら 2522
AWSImportExportFullAccess 2522
このポリシーを使用すると 2522
ポリシーの詳細 2523
ポリシーのバージョン 2523
JSON ポリシードキュメント 2523
詳細はこちら 2523
AWSImportExportReadOnlyAccess 2524
このポリシーを使用すると 2524
ポリシーの詳細 2524
ポリシーのバージョン 2524
JSON ポリシードキュメント 2524
詳細はこちら 2525
AWSIncidentManagerIncidentAccessServiceRolePolicy 2525
このポリシーを使用すると 2525
ポリシーの詳細 2525
ポリシーのバージョン 2525
JSON ポリシードキュメント 2526
詳細はこちら 2526

AWSIncidentManagerResolverAccess 2526
このポリシーを使用すると 2527
ポリシーの詳細 2527
ポリシーのバージョン 2527
JSON ポリシードキュメント 2527
詳細はこちら 2528
AWSIncidentManagerServiceRolePolicy 2528
このポリシーを使用すると 2529
ポリシーの詳細 2529
ポリシーのバージョン 2529
JSON ポリシードキュメント 2529
詳細はこちら 2530
AWSIoT1ClickFullAccess 2530
このポリシーを使用すると 2531
ポリシーの詳細 2531
ポリシーのバージョン 2531
JSON ポリシードキュメント 2531
詳細はこちら 2531
AWSIoT1ClickReadOnlyAccess 2532
このポリシーを使用すると 2532
ポリシーの詳細 2532
ポリシーのバージョン 2532
JSON ポリシードキュメント 2532
詳細はこちら 2533
AWSIoTAnalyticsFullAccess 2533
このポリシーを使用すると 2533
ポリシーの詳細 2533
ポリシーのバージョン 2533
JSON ポリシードキュメント 2534
詳細はこちら 2534
AWSIoTAnalyticsReadOnlyAccess 2534
このポリシーを使用すると 2534
ポリシーの詳細 2534
ポリシーのバージョン 2535
JSON ポリシードキュメント 2535
詳細はこちら 2535

AWSIoTConfigAccess 2535
このポリシーを使用すると 2536
ポリシーの詳細 2536
ポリシーのバージョン 2536
JSON ポリシードキュメント 2536
詳細はこちら 2540
AWSIoTConfigReadOnlyAccess 2540
このポリシーを使用すると 2540
ポリシーの詳細 2540
ポリシーのバージョン 2541
JSON ポリシードキュメント 2541
詳細はこちら 2543
AWSIoTDataAccess 2543
このポリシーを使用すると 2543
ポリシーの詳細 2543
ポリシーのバージョン 2543
JSON ポリシードキュメント 2544
詳細はこちら 2544
AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction 2544
このポリシーを使用すると 2545
ポリシーの詳細 2545
ポリシーのバージョン 2545
JSON ポリシードキュメント 2545
詳細はこちら 2546
AWSIoTDeviceDefenderAudit 2546
このポリシーを使用すると 2546
ポリシーの詳細 2546
ポリシーのバージョン 2546
JSON ポリシードキュメント 2546
詳細はこちら 2547
AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction 2548
このポリシーを使用すると 2548
ポリシーの詳細 2548
ポリシーのバージョン 2548
JSON ポリシードキュメント 2548
詳細はこちら 2549

AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction 2549
このポリシーを使用すると 2550
ポリシーの詳細 2550
ポリシーのバージョン 2550
JSON ポリシードキュメント 2550
詳細はこちら 2551
AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction 2551
このポリシーを使用すると 2551
ポリシーの詳細 2551
ポリシーのバージョン 2551
JSON ポリシードキュメント 2552
詳細はこちら 2552
AWSIoTDeviceDefenderUpdateCACertMitigationAction 2552
このポリシーを使用すると 2552
ポリシーの詳細 2552
ポリシーのバージョン 2553
JSON ポリシードキュメント 2553
詳細はこちら 2553
AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction 2554
このポリシーを使用すると 2554
ポリシーの詳細 2554
ポリシーのバージョン 2554
JSON ポリシードキュメント 2554
詳細はこちら 2555
AWSIoTDeviceTesterForFreeRTOSFullAccess 2555
このポリシーを使用すると 2555
ポリシーの詳細 2555
ポリシーのバージョン 2555
JSON ポリシードキュメント 2556
詳細はこちら 2562
AWSIoTDeviceTesterForGreengrassFullAccess 2562
このポリシーを使用すると 2562
ポリシーの詳細 2562
ポリシーのバージョン 2562
JSON ポリシードキュメント 2563
詳細はこちら 2566

AWSIoTEventsFullAccess 2566
このポリシーを使用すると 2566
ポリシーの詳細 2566
ポリシーのバージョン 2566
JSON ポリシードキュメント 2566
詳細はこちら 2567
AWSIoTEventsReadOnlyAccess 2567
このポリシーを使用すると 2567
ポリシーの詳細 2567
ポリシーのバージョン 2567
JSON ポリシードキュメント 2568
詳細はこちら 2568
AWSIoTFleetHubFederationAccess 2568
このポリシーを使用すると 2568
ポリシーの詳細 2569
ポリシーのバージョン 2569
JSON ポリシードキュメント 2569
詳細はこちら 2571
AWSIoTFleetwiseServiceRolePolicy 2571
このポリシーを使用すると 2571
ポリシーの詳細 2571
ポリシーのバージョン 2571
JSON ポリシードキュメント 2572
詳細はこちら 2572
AWSIoTFullAccess 2572
このポリシーを使用すると 2573
ポリシーの詳細 2573
ポリシーのバージョン 2573
JSON ポリシードキュメント 2573
詳細はこちら 2573
AWSIoTLogging 2574
このポリシーを使用すると 2574
ポリシーの詳細 2574
ポリシーのバージョン 2574
JSON ポリシードキュメント 2574
詳細はこちら 2575

AWSIoTManagedIntegrationsFullAccess 2575
このポリシーを使用すると 2575
ポリシーの詳細 2575
ポリシーのバージョン 2576
JSON ポリシードキュメント 2576
詳細はこちら 2576
AWSIoTManagedIntegrationsRolePolicy 2577
このポリシーを使用すると 2577
ポリシーの詳細 2577
ポリシーのバージョン 2577
JSON ポリシードキュメント 2577
詳細はこちら 2579
AWSIoTOTAUpdate 2579
このポリシーを使用すると 2579
ポリシーの詳細 2579
ポリシーのバージョン 2579
JSON ポリシードキュメント 2579
詳細はこちら 2580
AWSIotRoboRunnerFullAccess 2580
このポリシーを使用すると 2580
ポリシーの詳細 2580
ポリシーのバージョン 2580
JSON ポリシードキュメント 2581
詳細はこちら 2581
AWSIotRoboRunnerReadOnly 2581
このポリシーを使用すると 2582
ポリシーの詳細 2582
ポリシーのバージョン 2582
JSON ポリシードキュメント 2582
詳細はこちら 2583
AWSIotRoboRunnerServiceRolePolicy 2583
このポリシーを使用すると 2583
ポリシーの詳細 2583
ポリシーのバージョン 2583
JSON ポリシードキュメント 2584
詳細はこちら 2584

AWSIoTRuleActions 2584
このポリシーを使用すると 2584
ポリシーの詳細 2584
ポリシーのバージョン 2585
JSON ポリシードキュメント 2585
詳細はこちら 2585
AWSIoTSiteWiseConsoleFullAccess 2586
このポリシーを使用すると 2586
ポリシーの詳細 2586
ポリシーのバージョン 2586
JSON ポリシードキュメント 2586
詳細はこちら 2588
AWSIoTSiteWiseFullAccess 2589
このポリシーを使用すると 2589
ポリシーの詳細 2589
ポリシーのバージョン 2589
JSON ポリシードキュメント 2589
詳細はこちら 2590
AWSIoTSiteWiseMonitorPortalAccess 2590
このポリシーを使用すると 2590
ポリシーの詳細 2590
ポリシーのバージョン 2590
JSON ポリシードキュメント 2591
詳細はこちら 2592
AWSIoTSiteWiseMonitorServiceRolePolicy 2592
このポリシーを使用すると 2592
ポリシーの詳細 2592
ポリシーのバージョン 2592
JSON ポリシードキュメント 2593
詳細はこちら 2594
AWSIoTSiteWiseReadOnlyAccess 2594
このポリシーを使用すると 2594
ポリシーの詳細 2594
ポリシーのバージョン 2594
JSON ポリシードキュメント 2594
詳細はこちら 2596

AWSIoTThingsRegistration ... 2596
このポリシーを使用すると ... 2596
ポリシーの詳細 ... 2596
ポリシーのバージョン ... 2597
JSON ポリシードキュメント ... 2597
詳細はこちら ... 2598
AWSIoTTwinMakerServiceRolePolicy ... 2598
このポリシーを使用すると ... 2598
ポリシーの詳細 ... 2598
ポリシーのバージョン ... 2599
JSON ポリシードキュメント ... 2599
詳細はこちら ... 2600
AWSIoTWirelessDataAccess ... 2601
このポリシーを使用すると ... 2601
ポリシーの詳細 ... 2601
ポリシーのバージョン ... 2601
JSON ポリシードキュメント ... 2601
詳細はこちら ... 2602
AWSIoTWirelessFullAccess ... 2602
このポリシーを使用すると ... 2602
ポリシーの詳細 ... 2602
ポリシーのバージョン ... 2602
JSON ポリシードキュメント ... 2602
詳細はこちら ... 2603
AWSIoTWirelessFullPublishAccess ... 2603
このポリシーを使用すると ... 2603
ポリシーの詳細 ... 2603
ポリシーのバージョン ... 2604
JSON ポリシードキュメント ... 2604
詳細はこちら ... 2604
AWSIoTWirelessGatewayCertManager ... 2604
このポリシーを使用すると ... 2605
ポリシーの詳細 ... 2605
ポリシーのバージョン ... 2605
JSON ポリシードキュメント ... 2605
詳細はこちら ... 2606

AWSIoTWirelessLogging 2606
このポリシーを使用すると 2606
ポリシーの詳細 2606
ポリシーのバージョン 2606
JSON ポリシードキュメント 2606
詳細はこちら 2607
AWSIoTWirelessReadOnlyAccess 2607
このポリシーを使用すると 2607
ポリシーの詳細 2607
ポリシーのバージョン 2608
JSON ポリシードキュメント 2608
詳細はこちら 2608
AWSIPAMServiceRolePolicy 2608
このポリシーを使用すると 2609
ポリシーの詳細 2609
ポリシーのバージョン 2609
JSON ポリシードキュメント 2609
詳細はこちら 2611
AWSIQContractServiceRolePolicy 2611
このポリシーを使用すると 2611
ポリシーの詳細 2611
ポリシーのバージョン 2612
JSON ポリシードキュメント 2612
詳細はこちら 2612
AWSIQFullAccess 2612
このポリシーを使用すると 2613
ポリシーの詳細 2613
ポリシーのバージョン 2613
JSON ポリシードキュメント 2613
詳細はこちら 2614
AWSIQPermissionServiceRolePolicy 2614
このポリシーを使用すると 2614
ポリシーの詳細 2614
ポリシーのバージョン 2615
JSON ポリシードキュメント 2615
詳細はこちら 2616

AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy 2616
このポリシーを使用すると 2616
ポリシーの詳細 2616
ポリシーのバージョン 2616
JSON ポリシードキュメント 2617
詳細はこちら 2617
AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy 2617
このポリシーを使用すると 2618
ポリシーの詳細 2618
ポリシーのバージョン 2618
JSON ポリシードキュメント 2618
詳細はこちら 2619
AWSKeyManagementServicePowerUser 2619
このポリシーを使用すると 2619
ポリシーの詳細 2619
ポリシーのバージョン 2619
JSON ポリシードキュメント 2619
詳細はこちら 2620
AWSLakeFormationCrossAccountManager 2620
このポリシーを使用すると 2620
ポリシーの詳細 2621
ポリシーのバージョン 2621
JSON ポリシードキュメント 2621
詳細はこちら 2623
AWSLakeFormationDataAdmin 2623
このポリシーを使用すると 2623
ポリシーの詳細 2623
ポリシーのバージョン 2624
JSON ポリシードキュメント 2624
詳細はこちら 2625
AWSLambda_FullAccess 2625
このポリシーを使用すると 2626
ポリシーの詳細 2626
ポリシーのバージョン 2626
JSON ポリシードキュメント 2626
詳細はこちら 2628

AWSLambda_ReadOnlyAccess 2628
このポリシーを使用すると 2628
ポリシーの詳細 2628
ポリシーのバージョン 2628
JSON ポリシードキュメント 2629
詳細はこちら 2630
AWSLambdaBasicDurableExecutionRolePolicy 2630
このポリシーを使用すると 2630
ポリシーの詳細 2630
ポリシーのバージョン 2631
JSON ポリシードキュメント 2631
詳細はこちら 2631
AWSLambdaBasicExecutionRole 2631
このポリシーを使用すると 2632
ポリシーの詳細 2632
ポリシーのバージョン 2632
JSON ポリシードキュメント 2632
詳細はこちら 2632
AWSLambdaDynamoDBExecutionRole 2633
このポリシーを使用すると 2633
ポリシーの詳細 2633
ポリシーのバージョン 2633
JSON ポリシードキュメント 2633
詳細はこちら 2634
AWSLambdaENIManagementAccess 2634
このポリシーを使用すると 2634
ポリシーの詳細 2634
ポリシーのバージョン 2635
JSON ポリシードキュメント 2635
詳細はこちら 2635
AWSLambdaExecute 2635
このポリシーを使用すると 2636
ポリシーの詳細 2636
ポリシーのバージョン 2636
JSON ポリシードキュメント 2636
詳細はこちら 2637

AWSLambdaFullAccess 2637
このポリシーを使用すると 2637
ポリシーの詳細 2637
ポリシーのバージョン 2637
JSON ポリシードキュメント 2638
詳細はこちら 2639
AWSLambdaInvocation-DynamoDB 2639
このポリシーを使用すると 2640
ポリシーの詳細 2640
ポリシーのバージョン 2640
JSON ポリシードキュメント 2640
詳細はこちら 2641
AWSLambdaKinesisExecutionRole 2641
このポリシーを使用すると 2641
ポリシーの詳細 2641
ポリシーのバージョン 2641
JSON ポリシードキュメント 2642
詳細はこちら 2642
AWSLambdaManagedEC2ResourceOperator 2642
このポリシーを使用すると 2643
ポリシーの詳細 2643
ポリシーのバージョン 2643
JSON ポリシードキュメント 2643
詳細はこちら 2645
AWSLambdaMSKExecutionRole 2645
このポリシーを使用すると 2645
ポリシーの詳細 2645
ポリシーのバージョン 2645
JSON ポリシードキュメント 2646
詳細はこちら 2646
AWSLambdaReplicator 2646
このポリシーを使用すると 2647
ポリシーの詳細 2647
ポリシーのバージョン 2647
JSON ポリシードキュメント 2647
詳細はこちら 2648

AWSLambdaRole 2648
このポリシーを使用すると 2648
ポリシーの詳細 2649
ポリシーのバージョン 2649
JSON ポリシードキュメント 2649
詳細はこちら 2649
AWSLambdaServiceRolePolicy 2650
このポリシーを使用すると 2650
ポリシーの詳細 2650
ポリシーのバージョン 2650
JSON ポリシードキュメント 2650
詳細はこちら 2651
AWSLambdaSQSQueueExecutionRole 2651
このポリシーを使用すると 2651
ポリシーの詳細 2651
ポリシーのバージョン 2652
JSON ポリシードキュメント 2652
詳細はこちら 2652
AWSLambdaVPCAccessExecutionRole 2653
このポリシーを使用すると 2653
ポリシーの詳細 2653
ポリシーのバージョン 2653
JSON ポリシードキュメント 2653
詳細はこちら 2654
AWSLicenseManagerConsumptionPolicy 2654
このポリシーを使用すると 2654
ポリシーの詳細 2654
ポリシーのバージョン 2655
JSON ポリシードキュメント 2655
詳細はこちら 2655
AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy 2655
このポリシーを使用すると 2656
ポリシーの詳細 2656
ポリシーのバージョン 2656
JSON ポリシードキュメント 2656
詳細はこちら 2658

AWSLicenseManagerMasterAccountRolePolicy 2658
このポリシーを使用すると 2658
ポリシーの詳細 2658
ポリシーのバージョン 2659
JSON ポリシードキュメント 2659
詳細はこちら 2664
AWSLicenseManagerMemberAccountRolePolicy 2664
このポリシーを使用すると 2664
ポリシーの詳細 2664
ポリシーのバージョン 2664
JSON ポリシードキュメント 2664
詳細はこちら 2666
AWSLicenseManagerServiceRolePolicy 2666
このポリシーを使用すると 2666
ポリシーの詳細 2666
ポリシーのバージョン 2666
JSON ポリシードキュメント 2666
詳細はこちら 2670
AWSLicenseManagerUserSubscriptionsServiceRolePolicy 2670
このポリシーを使用すると 2670
ポリシーの詳細 2670
ポリシーのバージョン 2671
JSON ポリシードキュメント 2671
詳細はこちら 2674
AWSM2ServicePolicy 2674
このポリシーを使用すると 2674
ポリシーの詳細 2674
ポリシーのバージョン 2674
JSON ポリシードキュメント 2675
詳細はこちら 2676
AWSManagedServices_ContactsServiceRolePolicy 2676
このポリシーを使用すると 2676
ポリシーの詳細 2676
ポリシーのバージョン 2677
JSON ポリシードキュメント 2677
詳細はこちら 2678

AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy 2678
このポリシーを使用すると 2678
ポリシーの詳細 2678
ポリシーのバージョン 2678
JSON ポリシードキュメント 2679
詳細はこちら 2680
AWSManagedServices_EventsServiceRolePolicy 2680
このポリシーを使用すると 2680
ポリシーの詳細 2680
ポリシーのバージョン 2681
JSON ポリシードキュメント 2681
詳細はこちら 2682
AWSManagedServices_SelfServiceReporting_ServiceRolePolicy 2682
このポリシーを使用すると 2682
ポリシーの詳細 2682
ポリシーのバージョン 2682
JSON ポリシードキュメント 2683
詳細はこちら 2683
AWSManagedServicesDeploymentToolkitPolicy 2683
このポリシーを使用すると 2683
ポリシーの詳細 2683
ポリシーのバージョン 2684
JSON ポリシードキュメント 2684
詳細はこちら 2686
AWSManagementConsoleAdministratorAccess 2686
このポリシーを使用すると 2686
ポリシーの詳細 2686
ポリシーのバージョン 2687
JSON ポリシードキュメント 2687
詳細はこちら 2689
AWSManagementConsoleBasicUserAccess 2689
このポリシーを使用すると 2689
ポリシーの詳細 2690
ポリシーのバージョン 2690
JSON ポリシードキュメント 2690
詳細はこちら 2691

AWSMarketplaceAmiIngestion 2691
このポリシーを使用すると 2691
ポリシーの詳細 2691
ポリシーのバージョン 2692
JSON ポリシードキュメント 2692
詳細はこちら 2692
AWSMarketplaceDeploymentServiceRolePolicy 2693
このポリシーを使用すると 2693
ポリシーの詳細 2693
ポリシーのバージョン 2693
JSON ポリシードキュメント 2693
詳細はこちら 2695
AWSMarketplaceFullAccess 2695
このポリシーを使用すると 2695
ポリシーの詳細 2695
ポリシーのバージョン 2695
JSON ポリシードキュメント 2696
詳細はこちら 2697
AWSMarketplaceGetEntitlements 2698
このポリシーを使用すると 2698
ポリシーの詳細 2698
ポリシーのバージョン 2698
JSON ポリシードキュメント 2698
詳細はこちら 2699
AWSMarketplaceImageBuildFullAccess 2699
このポリシーを使用すると 2699
ポリシーの詳細 2699
ポリシーのバージョン 2699
JSON ポリシードキュメント 2700
詳細はこちら 2703
AWSMarketplaceLicenseManagementServiceRolePolicy 2703
このポリシーを使用すると 2704
ポリシーの詳細 2704
ポリシーのバージョン 2704
JSON ポリシードキュメント 2704
詳細はこちら 2705

AWSMarketplaceManageSubscriptions 2705
このポリシーを使用すると 2705
ポリシーの詳細 2705
ポリシーのバージョン 2705
JSON ポリシードキュメント 2706
詳細はこちら 2708
AWSMarketplaceMeteringFullAccess 2708
このポリシーを使用すると 2708
ポリシーの詳細 2708
ポリシーのバージョン 2708
JSON ポリシードキュメント 2709
詳細はこちら 2709
AWSMarketplaceMeteringRegisterUsage 2709
このポリシーを使用すると 2709
ポリシーの詳細 2709
ポリシーのバージョン 2710
JSON ポリシードキュメント 2710
詳細はこちら 2710
AWSMarketplaceProcurementSystemAdminFullAccess 2710
このポリシーを使用すると 2711
ポリシーの詳細 2711
ポリシーのバージョン 2711
JSON ポリシードキュメント 2711
詳細はこちら 2712
AWSMarketplacePurchaseOrdersServiceRolePolicy 2712
このポリシーを使用すると 2712
ポリシーの詳細 2712
ポリシーのバージョン 2712
JSON ポリシードキュメント 2713
詳細はこちら 2713
AWSMarketplaceRead-only 2713
このポリシーを使用すると 2713
ポリシーの詳細 2713
ポリシーのバージョン 2714
JSON ポリシードキュメント 2714
詳細はこちら 2715

AWSMarketplaceResaleAuthorizationServiceRolePolicy 2715
このポリシーを使用すると 2715
ポリシーの詳細 2716
ポリシーのバージョン 2716
JSON ポリシードキュメント 2716
詳細はこちら 2718
AWSMarketplaceSellerFullAccess 2718
このポリシーを使用すると 2719
ポリシーの詳細 2719
ポリシーのバージョン 2719
JSON ポリシードキュメント 2719
詳細はこちら 2723
AWSMarketplaceSellerOfferManagement 2723
このポリシーを使用すると 2723
ポリシーの詳細 2723
ポリシーのバージョン 2724
JSON ポリシードキュメント 2724
詳細はこちら 2726
AWSMarketplaceSellerProductsFullAccess 2726
このポリシーを使用すると 2726
ポリシーの詳細 2726
ポリシーのバージョン 2726
JSON ポリシードキュメント 2727
詳細はこちら 2730
AWSMarketplaceSellerProductsReadOnly 2730
このポリシーを使用すると 2730
ポリシーの詳細 2730
ポリシーのバージョン 2730
JSON ポリシードキュメント 2730
詳細はこちら 2731
AWSMcpServiceActionsFullAccess 2732
このポリシーを使用すると 2732
ポリシーの詳細 2732
ポリシーのバージョン 2732
JSON ポリシードキュメント 2732
詳細はこちら 2733

AWSMediaConnectServicePolicy 2733
このポリシーを使用すると 2733
ポリシーの詳細 2733
ポリシーのバージョン 2733
JSON ポリシードキュメント 2734
詳細はこちら 2735
AWSMediaLiveAnywhereServiceRolePolicy 2736
このポリシーを使用すると 2736
ポリシーの詳細 2736
ポリシーのバージョン 2736
JSON ポリシードキュメント 2736
詳細はこちら 2739
AWSMediaTailorServiceRolePolicy 2739
このポリシーを使用すると 2740
ポリシーの詳細 2740
ポリシーのバージョン 2740
JSON ポリシードキュメント 2740
詳細はこちら 2741
AWSMigrationHubDiscoveryAccess 2741
このポリシーを使用すると 2741
ポリシーの詳細 2741
ポリシーのバージョン 2741
JSON ポリシードキュメント 2742
詳細はこちら 2743
AWSMigrationHubDMSAccess 2743
このポリシーを使用すると 2743
ポリシーの詳細 2743
ポリシーのバージョン 2743
JSON ポリシードキュメント 2744
詳細はこちら 2745
AWSMigrationHubFullAccess 2745
このポリシーを使用すると 2745
ポリシーの詳細 2745
ポリシーのバージョン 2745
JSON ポリシードキュメント 2745
詳細はこちら 2747

AWSMigrationHubOrchestratorConsoleFullAccess 2747
このポリシーを使用すると 2747
ポリシーの詳細 2747
ポリシーのバージョン 2748
JSON ポリシードキュメント 2748
詳細はこちら 2751
AWSMigrationHubOrchestratorInstanceRolePolicy 2751
このポリシーを使用すると 2751
ポリシーの詳細 2751
ポリシーのバージョン 2752
JSON ポリシードキュメント 2752
詳細はこちら 2752
AWSMigrationHubOrchestratorPlugin 2753
このポリシーを使用すると 2753
ポリシーの詳細 2753
ポリシーのバージョン 2753
JSON ポリシードキュメント 2753
詳細はこちら 2754
AWSMigrationHubOrchestratorServiceRolePolicy 2755
このポリシーを使用すると 2755
ポリシーの詳細 2755
ポリシーのバージョン 2755
JSON ポリシードキュメント 2755
詳細はこちら 2759
AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess 2759
このポリシーを使用すると 2759
ポリシーの詳細 2759
ポリシーのバージョン 2760
JSON ポリシードキュメント 2760
詳細はこちら 2765
AWSMigrationHubRefactorSpaces-SSMAutomationPolicy 2766
このポリシーを使用すると 2766
ポリシーの詳細 2766
ポリシーのバージョン 2766
JSON ポリシードキュメント 2766
詳細はこちら 2768

AWSMigrationHubRefactorSpacesFullAccess 2768
このポリシーを使用すると 2768
ポリシーの詳細 2768
ポリシーのバージョン 2769
JSON ポリシードキュメント 2769
詳細はこちら 2775
AWSMigrationHubRefactorSpacesServiceRolePolicy 2775
このポリシーを使用すると 2776
ポリシーの詳細 2776
ポリシーのバージョン 2776
JSON ポリシードキュメント 2776
詳細はこちら 2780
AWSMigrationHubSMSAccess 2780
このポリシーを使用すると 2780
ポリシーの詳細 2780
ポリシーのバージョン 2780
JSON ポリシードキュメント 2781
詳細はこちら 2782
AWSMigrationHubStrategyCollector 2782
このポリシーを使用すると 2782
ポリシーの詳細 2782
ポリシーのバージョン 2782
JSON ポリシードキュメント 2783
詳細はこちら 2785
AWSMigrationHubStrategyConsoleFullAccess 2785
このポリシーを使用すると 2785
ポリシーの詳細 2785
ポリシーのバージョン 2786
JSON ポリシードキュメント 2786
詳細はこちら 2787
AWSMigrationHubStrategyServiceRolePolicy 2788
このポリシーを使用すると 2788
ポリシーの詳細 2788
ポリシーのバージョン 2788
JSON ポリシードキュメント 2788
詳細はこちら 2789

AWSMobileHub_FullAccess 2789
このポリシーを使用すると 2790
ポリシーの詳細 2790
ポリシーのバージョン 2790
JSON ポリシードキュメント 2790
詳細はこちら 2792
AWSMobileHub_ReadOnly 2792
このポリシーを使用すると 2792
ポリシーの詳細 2792
ポリシーのバージョン 2792
JSON ポリシードキュメント 2793
詳細はこちら 2794
AWSMSKReplicatorExecutionRole 2794
このポリシーを使用すると 2794
ポリシーの詳細 2794
ポリシーのバージョン 2794
JSON ポリシードキュメント 2795
詳細はこちら 2796
AWSNATGatewayServiceRolePolicy 2796
このポリシーを使用すると 2796
ポリシーの詳細 2796
ポリシーのバージョン 2797
JSON ポリシードキュメント 2797
詳細はこちら 2797
AWSNetworkFirewallFullAccess 2798
このポリシーを使用すると 2798
ポリシーの詳細 2798
ポリシーのバージョン 2798
JSON ポリシードキュメント 2798
詳細はこちら 2802
AWSNetworkFirewallReadOnlyAccess 2802
このポリシーを使用すると 2803
ポリシーの詳細 2803
ポリシーのバージョン 2803
JSON ポリシードキュメント 2803
詳細はこちら 2804

AWSNetworkFirewallServiceRolePolicy 2804
このポリシーを使用すると 2804
ポリシーの詳細 2805
ポリシーのバージョン 2805
JSON ポリシードキュメント 2805
詳細はこちら 2807
AWSNetworkManagerCloudWANServiceRolePolicy 2807
このポリシーを使用すると 2807
ポリシーの詳細 2807
ポリシーのバージョン 2807
JSON ポリシードキュメント 2807
詳細はこちら 2808
AWSNetworkManagerFullAccess 2808
このポリシーを使用すると 2808
ポリシーの詳細 2808
ポリシーのバージョン 2808
JSON ポリシードキュメント 2809
詳細はこちら 2809
AWSNetworkManagerReadOnlyAccess 2810
このポリシーを使用すると 2810
ポリシーの詳細 2810
ポリシーのバージョン 2810
JSON ポリシードキュメント 2810
詳細はこちら 2811
AWSNetworkManagerServiceRolePolicy 2811
このポリシーを使用すると 2811
ポリシーの詳細 2811
ポリシーのバージョン 2811
JSON ポリシードキュメント 2812
詳細はこちら 2813
AWSObservabilityAdminLogsCentralizationServiceRolePolicy 2813
このポリシーを使用すると 2813
ポリシーの詳細 2813
ポリシーのバージョン 2813
JSON ポリシードキュメント 2814
詳細はこちら 2814

AWSObservabilityAdminServiceRolePolicy 2815
このポリシーを使用すると 2815
ポリシーの詳細 2815
ポリシーのバージョン 2815
JSON ポリシードキュメント 2815
詳細はこちら 2818
AWSObservabilityAdminTelemetryEnablementServiceRolePolicy 2818
このポリシーを使用すると 2818
ポリシーの詳細 2818
ポリシーのバージョン 2819
JSON ポリシードキュメント 2819
詳細はこちら 2829
AWSOrganizationsFullAccess 2829
このポリシーを使用すると 2829
ポリシーの詳細 2829
ポリシーのバージョン 2829
JSON ポリシードキュメント 2829
詳細はこちら 2830
AWSOrganizationsReadOnlyAccess 2831
このポリシーを使用すると 2831
ポリシーの詳細 2831
ポリシーのバージョン 2831
JSON ポリシードキュメント 2831
詳細はこちら 2832
AWSOrganizationsServiceTrustPolicy 2832
このポリシーを使用すると 2832
ポリシーの詳細 2832
ポリシーのバージョン 2833
JSON ポリシードキュメント 2833
詳細はこちら 2833
AWSOutpostsAuthorizeServerPolicy 2834
このポリシーを使用すると 2834
ポリシーの詳細 2834
ポリシーのバージョン 2834
JSON ポリシードキュメント 2834
詳細はこちら 2835

AWSOutpostsServiceRolePolicy 2835
このポリシーを使用すると 2835
ポリシーの詳細 2835
ポリシーのバージョン 2835
JSON ポリシードキュメント 2836
詳細はこちら 2837
AWSPanoramaApplianceRolePolicy 2838
このポリシーを使用すると 2838
ポリシーの詳細 2838
ポリシーのバージョン 2838
JSON ポリシードキュメント 2838
詳細はこちら 2839
AWSPanoramaApplianceServiceRolePolicy 2839
このポリシーを使用すると 2839
ポリシーの詳細 2839
ポリシーのバージョン 2840
JSON ポリシードキュメント 2840
詳細はこちら 2841
AWSPanoramaFullAccess 2841
このポリシーを使用すると 2841
ポリシーの詳細 2842
ポリシーのバージョン 2842
JSON ポリシードキュメント 2842
詳細はこちら 2844
AWSPanoramaGreengrassGroupRolePolicy 2845
このポリシーを使用すると 2845
ポリシーの詳細 2845
ポリシーのバージョン 2845
JSON ポリシードキュメント 2845
詳細はこちら 2847
AWSPanoramaSageMakerRolePolicy 2847
このポリシーを使用すると 2847
ポリシーの詳細 2847
ポリシーのバージョン 2847
JSON ポリシードキュメント 2848
詳細はこちら 2848

AWSPanoramaServiceLinkedRolePolicy 2848
このポリシーを使用すると 2848
ポリシーの詳細 2849
ポリシーのバージョン 2849
JSON ポリシードキュメント 2849
詳細はこちら 2852
AWSPanoramaServiceRolePolicy 2852
このポリシーを使用すると 2852
ポリシーの詳細 2852
ポリシーのバージョン 2852
JSON ポリシードキュメント 2852
詳細はこちら 2859
AWSPartnerCentralChannelHandshakeApprovalManagement 2860
このポリシーを使用すると 2860
ポリシーの詳細 2860
ポリシーのバージョン 2860
JSON ポリシードキュメント 2860
詳細はこちら 2861
AWSPartnerCentralChannelManagement 2861
このポリシーを使用すると 2861
ポリシーの詳細 2861
ポリシーのバージョン 2862
JSON ポリシードキュメント 2862
詳細はこちら 2864
AWSPartnerCentralFullAccess 2864
このポリシーを使用すると 2865
ポリシーの詳細 2865
ポリシーのバージョン 2865
JSON ポリシードキュメント 2865
詳細はこちら 2868
AWSPartnerCentralMarketingManagement 2869
このポリシーを使用すると 2869
ポリシーの詳細 2869
ポリシーのバージョン 2869
JSON ポリシードキュメント 2869
詳細はこちら 2871

AWSPartnerCentralOpportunityManagement 2872
このポリシーを使用すると 2872
ポリシーの詳細 2872
ポリシーのバージョン 2872
JSON ポリシードキュメント 2872
詳細はこちら 2876
AWSPartnerCentralSandboxFullAccess 2876
このポリシーを使用すると 2876
ポリシーの詳細 2876
ポリシーのバージョン 2877
JSON ポリシードキュメント 2877
詳細はこちら 2878
AWSPartnerCentralSellingResourceSnapshotJobExecutionRolePolicy 2878
このポリシーを使用すると 2878
ポリシーの詳細 2878
ポリシーのバージョン 2878
JSON ポリシードキュメント 2879
詳細はこちら 2879
AWSPartnerLedSupportReadOnlyAccess 2880
このポリシーを使用すると 2880
ポリシーの詳細 2880
ポリシーのバージョン 2880
JSON ポリシードキュメント 2880
詳細はこちら 2917
AWSPCSComputeNodePolicy 2917
このポリシーを使用すると 2918
ポリシーの詳細 2918
ポリシーのバージョン 2918
JSON ポリシードキュメント 2918
詳細はこちら 2918
AWSPCSServiceRolePolicy 2919
このポリシーを使用すると 2919
ポリシーの詳細 2919
ポリシーのバージョン 2919
JSON ポリシードキュメント 2919
詳細はこちら 2924

AWSPriceListServiceFullAccess 2924
このポリシーを使用すると 2925
ポリシーの詳細 2925
ポリシーのバージョン 2925
JSON ポリシードキュメント 2925
詳細はこちら 2925
AWSPrivateCAAuditor 2926
このポリシーを使用すると 2926
ポリシーの詳細 2926
ポリシーのバージョン 2926
JSON ポリシードキュメント 2926
詳細はこちら 2927
AWSPrivateCAConnectorForKubernetesPolicy 2927
このポリシーを使用すると 2927
ポリシーの詳細 2928
ポリシーのバージョン 2928
JSON ポリシードキュメント 2928
詳細はこちら 2928
AWSPrivateCAFullAccess 2929
このポリシーを使用すると 2929
ポリシーの詳細 2929
ポリシーのバージョン 2929
JSON ポリシードキュメント 2929
詳細はこちら 2930
AWSPrivateCAPrivilegedUser 2930
このポリシーを使用すると 2930
ポリシーの詳細 2930
ポリシーのバージョン 2930
JSON ポリシードキュメント 2931
詳細はこちら 2932
AWSPrivateCAReadOnly 2932
このポリシーを使用すると 2932
ポリシーの詳細 2932
ポリシーのバージョン 2932
JSON ポリシードキュメント 2933
詳細はこちら 2933

AWSPrivateCAUser 2933
このポリシーを使用すると 2934
ポリシーの詳細 2934
ポリシーのバージョン 2934
JSON ポリシードキュメント 2934
詳細はこちら 2935
AWSPrivateMarketplaceAdminFullAccess 2935
このポリシーを使用すると 2936
ポリシーの詳細 2936
ポリシーのバージョン 2936
JSON ポリシードキュメント 2936
詳細はこちら 2939
AWSPrivateMarketplaceRequests 2939
このポリシーを使用すると 2939
ポリシーの詳細 2939
ポリシーのバージョン 2939
JSON ポリシードキュメント 2940
詳細はこちら 2941
AWSPrivateNetworksServiceRolePolicy 2942
このポリシーを使用すると 2942
ポリシーの詳細 2942
ポリシーのバージョン 2942
JSON ポリシードキュメント 2942
詳細はこちら 2943
AWSProtonCodeBuildProvisioningBasicAccess 2943
このポリシーを使用すると 2943
ポリシーの詳細 2943
ポリシーのバージョン 2944
JSON ポリシードキュメント 2944
詳細はこちら 2944
AWSProtonCodeBuildProvisioningServiceRolePolicy 2945
このポリシーを使用すると 2945
ポリシーの詳細 2945
ポリシーのバージョン 2945
JSON ポリシードキュメント 2945
詳細はこちら 2947

AWSProtonDeveloperAccess 2947
このポリシーを使用すると 2947
ポリシーの詳細 2947
ポリシーのバージョン 2947
JSON ポリシードキュメント 2947
詳細はこちら 2950
AWSProtonFullAccess 2950
このポリシーを使用すると 2950
ポリシーの詳細 2950
ポリシーのバージョン 2950
JSON ポリシードキュメント 2951
詳細はこちら 2953
AWSProtonReadOnlyAccess 2953
このポリシーを使用すると 2953
ポリシーの詳細 2953
ポリシーのバージョン 2953
JSON ポリシードキュメント 2954
詳細はこちら 2955
AWSProtonServiceGitSyncServiceRolePolicy 2955
このポリシーを使用すると 2955
ポリシーの詳細 2955
ポリシーのバージョン 2956
JSON ポリシードキュメント 2956
詳細はこちら 2957
AWSProtonSyncServiceRolePolicy 2957
このポリシーを使用すると 2957
ポリシーの詳細 2957
ポリシーのバージョン 2957
JSON ポリシードキュメント 2958
詳細はこちら 2959
AWSPurchaseOrdersServiceRolePolicy 2959
このポリシーを使用すると 2959
ポリシーの詳細 2959
ポリシーのバージョン 2959
JSON ポリシードキュメント 2959
詳細はこちら 2960

AWSQuickSetupCFGCPacksPermissionsBoundary 2961
このポリシーを使用すると 2961
ポリシーの詳細 2961
ポリシーのバージョン 2961
JSON ポリシードキュメント 2961
詳細はこちら 2964
AWSQuickSetupDeploymentRolePolicy 2964
このポリシーを使用すると 2965
ポリシーの詳細 2965
ポリシーのバージョン 2965
JSON ポリシードキュメント 2965
詳細はこちら 2973
AWSQuickSetupDevOpsGuruPermissionsBoundary 2974
このポリシーを使用すると 2974
ポリシーの詳細 2974
ポリシーのバージョン 2974
JSON ポリシードキュメント 2974
詳細はこちら 2977
AWSQuickSetupDistributorPermissionsBoundary 2977
このポリシーを使用すると 2977
ポリシーの詳細 2978
ポリシーのバージョン 2978
JSON ポリシードキュメント 2978
詳細はこちら 2984
AWSQuickSetupEnableAREXExecutionPolicy 2984
このポリシーを使用すると 2984
ポリシーの詳細 2984
ポリシーのバージョン 2984
JSON ポリシードキュメント 2985
詳細はこちら 2986
AWSQuickSetupEnableDHMCExecutionPolicy 2986
このポリシーを使用すると 2987
ポリシーの詳細 2987
ポリシーのバージョン 2987
JSON ポリシードキュメント 2987
詳細はこちら 2988

AWSQuickSetupJITNADeploymentRolePolicy 2988
このポリシーを使用すると 2989
ポリシーの詳細 2989
ポリシーのバージョン 2989
JSON ポリシードキュメント 2989
詳細はこちら 2993
AWSQuickSetupManagedInstanceProfileExecutionPolicy 2993
このポリシーを使用すると 2993
ポリシーの詳細 2993
ポリシーのバージョン 2993
JSON ポリシードキュメント 2994
詳細はこちら 2998
AWSQuickSetupManageJITNAResourcesExecutionPolicy 2998
このポリシーを使用すると 2998
ポリシーの詳細 2998
ポリシーのバージョン 2998
JSON ポリシードキュメント 2999
詳細はこちら 3001
AWSQuickSetupPatchPolicyBaselineAccess 3001
このポリシーを使用すると 3001
ポリシーの詳細 3001
ポリシーのバージョン 3001
JSON ポリシードキュメント 3002
詳細はこちら 3002
AWSQuickSetupPatchPolicyDeploymentRolePolicy 3003
このポリシーを使用すると 3003
ポリシーの詳細 3003
ポリシーのバージョン 3003
JSON ポリシードキュメント 3003
詳細はこちら 3011
AWSQuickSetupPatchPolicyPermissionsBoundary 3012
このポリシーを使用すると 3012
ポリシーの詳細 3012
ポリシーのバージョン 3012
JSON ポリシードキュメント 3012
詳細はこちら 3020

AWSQuickSetupSchedulerPermissionsBoundary 3021
このポリシーを使用すると 3021
ポリシーの詳細 3021
ポリシーのバージョン 3021
JSON ポリシードキュメント 3021
詳細はこちら 3025
AWSQuickSetupSSMDeploymentRolePolicy 3025
このポリシーを使用すると 3025
ポリシーの詳細 3025
ポリシーのバージョン 3025
JSON ポリシードキュメント 3025
詳細はこちら 3036
AWSQuickSetupSSMDeploymentS3BucketRolePolicy 3036
このポリシーを使用すると 3036
ポリシーの詳細 3037
ポリシーのバージョン 3037
JSON ポリシードキュメント 3037
詳細はこちら 3038
AWSQuickSetupSSMHostMgmtPermissionsBoundary 3038
このポリシーを使用すると 3038
ポリシーの詳細 3038
ポリシーのバージョン 3038
JSON ポリシードキュメント 3039
詳細はこちら 3044
AWSQuickSetupSSMLifecycleManagementExecutionPolicy 3045
このポリシーを使用すると 3045
ポリシーの詳細 3045
ポリシーのバージョン 3045
JSON ポリシードキュメント 3045
詳細はこちら 3047
AWSQuickSetupSSMManageResourcesExecutionPolicy 3047
このポリシーを使用すると 3047
ポリシーの詳細 3047
ポリシーのバージョン 3047
JSON ポリシードキュメント 3048
詳細はこちら 3050

AWSQuickSetupStartSSMAssociationsExecutionPolicy 3051
このポリシーを使用すると 3051
ポリシーの詳細 3051
ポリシーのバージョン 3051
JSON ポリシードキュメント 3051
詳細はこちら 3052
AWSQuickSetupStartStopInstancesExecutionPolicy 3053
このポリシーを使用すると 3053
ポリシーの詳細 3053
ポリシーのバージョン 3053
JSON ポリシードキュメント 3053
詳細はこちら 3055
AWSQuickSightAssetBundleExportPolicy 3055
このポリシーを使用すると 3055
ポリシーの詳細 3055
ポリシーのバージョン 3056
JSON ポリシードキュメント 3056
詳細はこちら 3058
AWSQuickSightAssetBundleImportPolicy 3058
このポリシーを使用すると 3058
ポリシーの詳細 3058
ポリシーのバージョン 3059
JSON ポリシードキュメント 3059
詳細はこちら 3062
AWSQuicksightAthenaAccess 3062
このポリシーを使用すると 3062
ポリシーの詳細 3062
ポリシーのバージョン 3062
JSON ポリシードキュメント 3062
詳細はこちら 3065
AWSQuickSightDescribeRDS 3065
このポリシーを使用すると 3065
ポリシーの詳細 3065
ポリシーのバージョン 3065
JSON ポリシードキュメント 3066
詳細はこちら 3066

AWSQuickSightDescribeRedshift 3066
このポリシーを使用すると 3066
ポリシーの詳細 3066
ポリシーのバージョン 3067
JSON ポリシードキュメント 3067
詳細はこちら 3067
AWSQuickSightElasticsearchPolicy 3067
このポリシーを使用すると 3068
ポリシーの詳細 3068
ポリシーのバージョン 3068
JSON ポリシードキュメント 3068
詳細はこちら 3069
AWSQuickSightIoTAnalyticsAccess 3069
このポリシーを使用すると 3070
ポリシーの詳細 3070
ポリシーのバージョン 3070
JSON ポリシードキュメント 3070
詳細はこちら 3071
AWSQuickSightListIAM 3071
このポリシーを使用すると 3071
ポリシーの詳細 3071
ポリシーのバージョン 3071
JSON ポリシードキュメント 3071
詳細はこちら 3072
AWSQuicksightOpenSearchPolicy 3072
このポリシーを使用すると 3072
ポリシーの詳細 3072
ポリシーのバージョン 3072
JSON ポリシードキュメント 3073
詳細はこちら 3074
AWSQuickSightSageMakerPolicy 3074
このポリシーを使用すると 3074
ポリシーの詳細 3074
ポリシーのバージョン 3074
JSON ポリシードキュメント 3075
詳細はこちら 3076

AWSQuickSightSecretsManagerWriteAccess 3076
このポリシーを使用すると 3076
ポリシーの詳細 3076
ポリシーのバージョン 3077
JSON ポリシードキュメント 3077
詳細はこちら 3078
AWSQuickSightSecretsManagerWritePolicy 3078
このポリシーを使用すると 3078
ポリシーの詳細 3078
ポリシーのバージョン 3078
JSON ポリシードキュメント 3079
詳細はこちら 3079
AWSQuickSightTimestreamPolicy 3080
このポリシーを使用すると 3080
ポリシーの詳細 3080
ポリシーのバージョン 3080
JSON ポリシードキュメント 3080
詳細はこちら 3081
AWSReachabilityAnalyzerServiceRolePolicy 3081
このポリシーを使用すると 3081
ポリシーの詳細 3081
ポリシーのバージョン 3082
JSON ポリシードキュメント 3082
詳細はこちら 3084
AWSRefactoringToolkitFullAccess 3084
このポリシーを使用すると 3084
ポリシーの詳細 3085
ポリシーのバージョン 3085
JSON ポリシードキュメント 3085
詳細はこちら 3098
AWSRefactoringToolkitSidecarPolicy 3099
このポリシーを使用すると 3099
ポリシーの詳細 3099
ポリシーのバージョン 3099
JSON ポリシードキュメント 3099
詳細はこちら 3100

AWSrePostPrivateCloudWatchAccess 3101
このポリシーを使用すると 3101
ポリシーの詳細 3101
ポリシーのバージョン 3101
JSON ポリシードキュメント 3101
詳細はこちら 3102
AWSRepostSpaceSupportOperationsPolicy 3102
このポリシーを使用すると 3102
ポリシーの詳細 3102
ポリシーのバージョン 3103
JSON ポリシードキュメント 3103
詳細はこちら 3103
AWSResilienceHubAsssessmentExecutionPolicy 3104
このポリシーを使用すると 3104
ポリシーの詳細 3104
ポリシーのバージョン 3104
JSON ポリシードキュメント 3104
詳細はこちら 3109
AWSResourceAccessManagerFullAccess 3109
このポリシーを使用すると 3109
ポリシーの詳細 3109
ポリシーのバージョン 3110
JSON ポリシードキュメント 3110
詳細はこちら 3110
AWSResourceAccessManagerReadOnlyAccess 3110
このポリシーを使用すると 3111
ポリシーの詳細 3111
ポリシーのバージョン 3111
JSON ポリシードキュメント 3111
詳細はこちら 3111
AWSResourceAccessManagerResourceShareParticipantAccess 3112
このポリシーを使用すると 3112
ポリシーの詳細 3112
ポリシーのバージョン 3112
JSON ポリシードキュメント 3112
詳細はこちら 3113

AWSResourceAccessManagerServiceRolePolicy 3113
このポリシーを使用すると 3113
ポリシーの詳細 3113
ポリシーのバージョン 3114
JSON ポリシードキュメント 3114
詳細はこちら 3115
AWSResourceExplorerFullAccess 3115
このポリシーを使用すると 3115
ポリシーの詳細 3115
ポリシーのバージョン 3115
JSON ポリシードキュメント 3116
詳細はこちら 3116
AWSResourceExplorerOrganizationsAccess 3117
このポリシーを使用すると 3117
ポリシーの詳細 3117
ポリシーのバージョン 3117
JSON ポリシードキュメント 3117
詳細はこちら 3119
AWSResourceExplorerReadOnlyAccess 3119
このポリシーを使用すると 3119
ポリシーの詳細 3119
ポリシーのバージョン 3120
JSON ポリシードキュメント 3120
詳細はこちら 3120
AWSResourceExplorerServiceRolePolicy 3121
このポリシーを使用すると 3121
ポリシーの詳細 3121
ポリシーのバージョン 3121
JSON ポリシードキュメント 3121
詳細はこちら 3140
AWSResourceGroupsReadOnlyAccess 3140
このポリシーを使用すると 3141
ポリシーの詳細 3141
ポリシーのバージョン 3141
JSON ポリシードキュメント 3141
詳細はこちら 3142

AWSRoboMaker_FullAccess 3143
このポリシーを使用すると 3143
ポリシーの詳細 3143
ポリシーのバージョン 3143
JSON ポリシードキュメント 3143
詳細はこちら 3145
AWSRoboMakerReadOnlyAccess 3145
このポリシーを使用すると 3145
ポリシーの詳細 3145
ポリシーのバージョン 3145
JSON ポリシードキュメント 3145
詳細はこちら 3146
AWSRoboMakerServicePolicy 3146
このポリシーを使用すると 3146
ポリシーの詳細 3146
ポリシーのバージョン 3147
JSON ポリシードキュメント 3147
詳細はこちら 3148
AWSRoboMakerServiceRolePolicy 3149
このポリシーを使用すると 3149
ポリシーの詳細 3149
ポリシーのバージョン 3149
JSON ポリシードキュメント 3149
詳細はこちら 3150
AWSRolesAnywhereFullAccess 3151
このポリシーを使用すると 3151
ポリシーの詳細 3151
ポリシーのバージョン 3151
JSON ポリシードキュメント 3151
詳細はこちら 3154
AWSRolesAnywhereReadOnly 3154
このポリシーを使用すると 3154
ポリシーの詳細 3154
ポリシーのバージョン 3154
JSON ポリシードキュメント 3155
詳細はこちら 3156

AWSRolesAnywhereServicePolicy 3156
このポリシーを使用すると 3156
ポリシーの詳細 3157
ポリシーのバージョン 3157
JSON ポリシードキュメント 3157
詳細はこちら 3158
AWSS3OnOutpostsServiceRolePolicy 3158
このポリシーを使用すると 3158
ポリシーの詳細 3158
ポリシーのバージョン 3158
JSON ポリシードキュメント 3159
詳細はこちら 3161
AWSSavingsPlansFullAccess 3161
このポリシーを使用すると 3162
ポリシーの詳細 3162
ポリシーのバージョン 3162
JSON ポリシードキュメント 3162
詳細はこちら 3162
AWSSavingsPlansReadOnlyAccess 3163
このポリシーを使用すると 3163
ポリシーの詳細 3163
ポリシーのバージョン 3163
JSON ポリシードキュメント 3163
詳細はこちら 3164
AWSSecretsManagerClientReadOnlyAccess 3164
このポリシーを使用すると 3164
ポリシーの詳細 3164
ポリシーのバージョン 3164
JSON ポリシードキュメント 3164
詳細はこちら 3165
AWSSecurityHubFullAccess 3165
このポリシーを使用すると 3166
ポリシーの詳細 3166
ポリシーのバージョン 3166
JSON ポリシードキュメント 3166
詳細はこちら 3167

AWSSecurityHubOrganizationsAccess 3168
このポリシーを使用すると 3168
ポリシーの詳細 3168
ポリシーのバージョン 3168
JSON ポリシードキュメント 3168
詳細はこちら 3171
AWSSecurityHubReadOnlyAccess 3171
このポリシーを使用すると 3171
ポリシーの詳細 3171
ポリシーのバージョン 3171
JSON ポリシードキュメント 3172
詳細はこちら 3172
AWSSecurityHubServiceRolePolicy 3172
このポリシーを使用すると 3173
ポリシーの詳細 3173
ポリシーのバージョン 3173
JSON ポリシードキュメント 3173
詳細はこちら 3175
AWSSecurityHubV2ServiceRolePolicy 3175
このポリシーを使用すると 3175
ポリシーの詳細 3176
ポリシーのバージョン 3176
JSON ポリシードキュメント 3176
詳細はこちら 3179
AWSSecurityIncidentResponseCaseFullAccess 3179
このポリシーを使用すると 3179
ポリシーの詳細 3179
ポリシーのバージョン 3180
JSON ポリシードキュメント 3180
詳細はこちら 3181
AWSSecurityIncidentResponseFullAccess 3182
このポリシーを使用すると 3182
ポリシーの詳細 3182
ポリシーのバージョン 3182
JSON ポリシードキュメント 3182
詳細はこちら 3184

AWSSecurityIncidentResponseReadOnlyAccess 3185
このポリシーを使用すると 3185
ポリシーの詳細 3185
ポリシーのバージョン 3185
JSON ポリシードキュメント 3185
詳細はこちら 3186
AWSSecurityIncidentResponseServiceRolePolicy 3186
このポリシーを使用すると 3186
ポリシーの詳細 3186
ポリシーのバージョン 3187
JSON ポリシードキュメント 3187
詳細はこちら 3188
AWSSecurityIncidentResponseTriageServiceRolePolicy 3188
このポリシーを使用すると 3189
ポリシーの詳細 3189
ポリシーのバージョン 3189
JSON ポリシードキュメント 3189
詳細はこちら 3191
AWSServiceCatalogAdminFullAccess 3192
このポリシーを使用すると 3192
ポリシーの詳細 3192
ポリシーのバージョン 3192
JSON ポリシードキュメント 3192
詳細はこちら 3195
AWSServiceCatalogAdminReadOnlyAccess 3195
このポリシーを使用すると 3195
ポリシーの詳細 3195
ポリシーのバージョン 3196
JSON ポリシードキュメント 3196
詳細はこちら 3197
AWSServiceCatalogAppRegistryFullAccess 3197
このポリシーを使用すると 3197
ポリシーの詳細 3197
ポリシーのバージョン 3198
JSON ポリシードキュメント 3198
詳細はこちら 3200

AWSServiceCatalogAppRegistryReadOnlyAccess 3200
このポリシーを使用すると 3200
ポリシーの詳細 3201
ポリシーのバージョン 3201
JSON ポリシードキュメント 3201
詳細はこちら 3202
AWSServiceCatalogAppRegistryServiceRolePolicy 3202
このポリシーを使用すると 3202
ポリシーの詳細 3202
ポリシーのバージョン 3202
JSON ポリシードキュメント 3203
詳細はこちら 3204
AWSServiceCatalogEndUserFullAccess 3204
このポリシーを使用すると 3204
ポリシーの詳細 3204
ポリシーのバージョン 3204
JSON ポリシードキュメント 3205
詳細はこちら 3207
AWSServiceCatalogEndUserReadOnlyAccess 3207
このポリシーを使用すると 3207
ポリシーの詳細 3207
ポリシーのバージョン 3207
JSON ポリシードキュメント 3208
詳細はこちら 3209
AWSServiceCatalogOrgsDataSyncServiceRolePolicy 3209
このポリシーを使用すると 3210
ポリシーの詳細 3210
ポリシーのバージョン 3210
JSON ポリシードキュメント 3210
詳細はこちら 3211
AWSServiceCatalogSyncServiceRolePolicy 3211
このポリシーを使用すると 3211
ポリシーの詳細 3211
ポリシーのバージョン 3212
JSON ポリシードキュメント 3212
詳細はこちら 3213

AWSServiceRoleForAmazonEKSNodegroup 3213
このポリシーを使用すると 3213
ポリシーの詳細 3213
ポリシーのバージョン 3214
JSON ポリシードキュメント 3214
詳細はこちら 3219
AWSServiceRoleForAmazonQDeveloper 3219
このポリシーを使用すると 3220
ポリシーの詳細 3220
ポリシーのバージョン 3220
JSON ポリシードキュメント 3220
詳細はこちら 3221
AWSServiceRoleForAWSTransform 3221
このポリシーを使用すると 3221
ポリシーの詳細 3221
ポリシーのバージョン 3221
JSON ポリシードキュメント 3222
詳細はこちら 3224
AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy 3224
このポリシーを使用すると 3224
ポリシーの詳細 3224
ポリシーのバージョン 3225
JSON ポリシードキュメント 3225
詳細はこちら 3225
AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy 3225
このポリシーを使用すると 3226
ポリシーの詳細 3226
ポリシーのバージョン 3226
JSON ポリシードキュメント 3226
詳細はこちら 3227
AWSServiceRoleForCodeGuru-Profiler 3227
このポリシーを使用すると 3227
ポリシーの詳細 3227
ポリシーのバージョン 3227
JSON ポリシードキュメント 3228
詳細はこちら 3228

AWSServiceRoleForCodeWhispererPolicy 3228
このポリシーを使用すると 3228
ポリシーの詳細 3228
ポリシーのバージョン 3229
JSON ポリシードキュメント 3229
詳細はこちら 3231
AWSServiceRoleForEC2ScheduledInstances 3231
このポリシーを使用すると 3231
ポリシーの詳細 3231
ポリシーのバージョン 3231
JSON ポリシードキュメント 3232
詳細はこちら 3232
AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy 3233
このポリシーを使用すると 3233
ポリシーの詳細 3233
ポリシーのバージョン 3233
JSON ポリシードキュメント 3233
詳細はこちら 3234
AWSServiceRoleForImageBuilder 3234
このポリシーを使用すると 3234
ポリシーの詳細 3234
ポリシーのバージョン 3234
JSON ポリシードキュメント 3235
詳細はこちら 3245
AWSServiceRoleForIoTSiteWise 3245
このポリシーを使用すると 3246
ポリシーの詳細 3246
ポリシーのバージョン 3246
JSON ポリシードキュメント 3246
詳細はこちら 3247
AWSServiceRoleForLogDeliveryPolicy 3248
このポリシーを使用すると 3248
ポリシーの詳細 3248
ポリシーのバージョン 3248
JSON ポリシードキュメント 3248
詳細はこちら 3249

AWSServiceRoleForMonitronPolicy 3249
このポリシーを使用すると 3249
ポリシーの詳細 3249
ポリシーのバージョン 3250
JSON ポリシードキュメント 3250
詳細はこちら 3250
AWSServiceRoleForNeptuneGraphPolicy 3251
このポリシーを使用すると 3251
ポリシーの詳細 3251
ポリシーのバージョン 3251
JSON ポリシードキュメント 3251
詳細はこちら 3253
AWSServiceRoleForPrivateMarketplaceAdminPolicy 3253
このポリシーを使用すると 3253
ポリシーの詳細 3253
ポリシーのバージョン 3253
JSON ポリシードキュメント 3254
詳細はこちら 3255
AWSServiceRoleForProcurementInsightsPolicy 3255
このポリシーを使用すると 3256
ポリシーの詳細 3256
ポリシーのバージョン 3256
JSON ポリシードキュメント 3256
詳細はこちら 3257
AWSServiceRoleForSMS 3257
このポリシーを使用すると 3257
ポリシーの詳細 3257
ポリシーのバージョン 3257
JSON ポリシードキュメント 3258
詳細はこちら 3264
AWSServiceRoleForUserSubscriptions 3264
このポリシーを使用すると 3265
ポリシーの詳細 3265
ポリシーのバージョン 3265
JSON ポリシードキュメント 3265
詳細はこちら 3267

AWSServiceRolePolicyForBackupReports 3267
このポリシーを使用すると 3267
ポリシーの詳細 3267
ポリシーのバージョン 3267
JSON ポリシードキュメント 3267
詳細はこちら 3269
AWSServiceRolePolicyForBackupRestoreTesting 3269
このポリシーを使用すると 3269
ポリシーの詳細 3269
ポリシーのバージョン 3269
JSON ポリシードキュメント 3270
詳細はこちら 3272
AWSServiceRolePolicyForWorkspacesInstances 3273
このポリシーを使用すると 3273
ポリシーの詳細 3273
ポリシーのバージョン 3273
JSON ポリシードキュメント 3273
詳細はこちら 3274
AWSShieldDRTAccessPolicy 3274
このポリシーを使用すると 3274
ポリシーの詳細 3274
ポリシーのバージョン 3275
JSON ポリシードキュメント 3275
詳細はこちら 3276
AWSShieldServiceRolePolicy 3276
このポリシーを使用すると 3276
ポリシーの詳細 3276
ポリシーのバージョン 3277
JSON ポリシードキュメント 3277
詳細はこちら 3277
AWSSocialMessagingServiceRolePolicy 3277
このポリシーを使用すると 3278
ポリシーの詳細 3278
ポリシーのバージョン 3278
JSON ポリシードキュメント 3278
詳細はこちら 3279

AWSSSMForSAPServiceLinkedRolePolicy 3279
このポリシーを使用すると 3279
ポリシーの詳細 3279
ポリシーのバージョン 3279
JSON ポリシードキュメント 3280
詳細はこちら 3288
AWSSSMOpsInsightsServiceRolePolicy 3288
このポリシーを使用すると 3288
ポリシーの詳細 3288
ポリシーのバージョン 3289
JSON ポリシードキュメント 3289
詳細はこちら 3290
AWSSSODirectoryAdministrator 3290
このポリシーを使用すると 3290
ポリシーの詳細 3290
ポリシーのバージョン 3290
JSON ポリシードキュメント 3290
詳細はこちら 3291
AWSSSODirectoryReadOnly 3291
このポリシーを使用すると 3292
ポリシーの詳細 3292
ポリシーのバージョン 3292
JSON ポリシードキュメント 3292
詳細はこちら 3293
AWSSSOMasterAccountAdministrator 3293
このポリシーを使用すると 3293
ポリシーの詳細 3293
ポリシーのバージョン 3294
JSON ポリシードキュメント 3294
詳細はこちら 3297
AWSSSOMemberAccountAdministrator 3297
このポリシーを使用すると 3297
ポリシーの詳細 3297
ポリシーのバージョン 3297
JSON ポリシードキュメント 3298
詳細はこちら 3300

AWSSSOReadOnly 3300
このポリシーを使用すると 3300
ポリシーの詳細 3300
ポリシーのバージョン 3300
JSON ポリシードキュメント 3301
詳細はこちら 3302
AWSSSOServiceRolePolicy 3302
このポリシーを使用すると 3302
ポリシーの詳細 3303
ポリシーのバージョン 3303
JSON ポリシードキュメント 3303
詳細はこちら 3307
AWSStepFunctionsConsoleFullAccess 3307
このポリシーを使用すると 3307
ポリシーの詳細 3307
ポリシーのバージョン 3307
JSON ポリシードキュメント 3308
詳細はこちら 3308
AWSStepFunctionsFullAccess 3309
このポリシーを使用すると 3309
ポリシーの詳細 3309
ポリシーのバージョン 3309
JSON ポリシードキュメント 3309
詳細はこちら 3310
AWSStepFunctionsReadOnlyAccess 3310
このポリシーを使用すると 3310
ポリシーの詳細 3310
ポリシーのバージョン 3310
JSON ポリシードキュメント 3311
詳細はこちら 3311
AWSStorageGatewayFullAccess 3311
このポリシーを使用すると 3312
ポリシーの詳細 3312
ポリシーのバージョン 3312
JSON ポリシードキュメント 3312
詳細はこちら 3313

AWSStorageGatewayReadOnlyAccess 3313
このポリシーを使用すると 3313
ポリシーの詳細 3313
ポリシーのバージョン 3313
JSON ポリシードキュメント 3314
詳細はこちら 3314
AWSStorageGatewayServiceRolePolicy 3315
このポリシーを使用すると 3315
ポリシーの詳細 3315
ポリシーのバージョン 3315
JSON ポリシードキュメント 3315
詳細はこちら 3316
AWSSupplyChainFederationAdminAccess 3316
このポリシーを使用すると 3316
ポリシーの詳細 3316
ポリシーのバージョン 3316
JSON ポリシードキュメント 3317
詳細はこちら 3323
AWSSupportAccess 3323
このポリシーを使用すると 3323
ポリシーの詳細 3323
ポリシーのバージョン 3323
JSON ポリシードキュメント 3324
詳細はこちら 3324
AWSSupportAppFullAccess 3324
このポリシーを使用すると 3324
ポリシーの詳細 3325
ポリシーのバージョン 3325
JSON ポリシードキュメント 3325
詳細はこちら 3326
AWSSupportAppReadOnlyAccess 3326
このポリシーを使用すると 3326
ポリシーの詳細 3326
ポリシーのバージョン 3326
JSON ポリシードキュメント 3327
詳細はこちら 3327

AWSSupportPlansFullAccess 3327
このポリシーを使用すると 3327
ポリシーの詳細 3328
ポリシーのバージョン 3328
JSON ポリシードキュメント 3328
詳細はこちら 3328
AWSSupportPlansReadOnlyAccess 3329
このポリシーを使用すると 3329
ポリシーの詳細 3329
ポリシーのバージョン 3329
JSON ポリシードキュメント 3329
詳細はこちら 3330
AWSSupportServiceRolePolicy 3330
このポリシーを使用すると 3330
ポリシーの詳細 3330
ポリシーのバージョン 3330
JSON ポリシードキュメント 3331
詳細はこちら 3423
AWSSystemsManagerAccountDiscoveryServicePolicy 3423
このポリシーを使用すると 3423
ポリシーの詳細 3423
ポリシーのバージョン 3423
JSON ポリシードキュメント 3424
詳細はこちら 3424
AWSSystemsManagerChangeManagementServicePolicy 3424
このポリシーを使用すると 3425
ポリシーの詳細 3425
ポリシーのバージョン 3425
JSON ポリシードキュメント 3425
詳細はこちら 3428
AWSSystemsManagerEnableConfigRecordingExecutionPolicy 3428
このポリシーを使用すると 3428
ポリシーの詳細 3428
ポリシーのバージョン 3428
JSON ポリシードキュメント 3428
詳細はこちら 3430

AWSSystemsManagerEnableExplorerExecutionPolicy 3431
このポリシーを使用すると 3431
ポリシーの詳細 3431
ポリシーのバージョン 3431
JSON ポリシードキュメント 3431
詳細はこちら 3433
AWSSystemsManagerForSAPFullAccess 3433
このポリシーを使用すると 3433
ポリシーの詳細 3433
ポリシーのバージョン 3433
JSON ポリシードキュメント 3433
詳細はこちら 3435
AWSSystemsManagerForSAPReadOnlyAccess 3435
このポリシーを使用すると 3435
ポリシーの詳細 3435
ポリシーのバージョン 3435
JSON ポリシードキュメント 3435
詳細はこちら 3436
AWSSystemsManagerJustInTimeAccessServicePolicy 3436
このポリシーを使用すると 3436
ポリシーの詳細 3436
ポリシーのバージョン 3437
JSON ポリシードキュメント 3437
詳細はこちら 3442
AWSSystemsManagerJustInTimeAccessTokenPolicy 3442
このポリシーを使用すると 3442
ポリシーの詳細 3443
ポリシーのバージョン 3443
JSON ポリシードキュメント 3443
詳細はこちら 3446
AWSSystemsManagerJustInTimeAccessTokenSessionPolicy 3446
このポリシーを使用すると 3446
ポリシーの詳細 3446
ポリシーのバージョン 3447
JSON ポリシードキュメント 3447
詳細はこちら 3449

AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy 3449
このポリシーを使用すると 3450
ポリシーの詳細 3450
ポリシーのバージョン 3450
JSON ポリシードキュメント 3450
詳細はこちら 3454
AWSSystemsManagerNotificationsServicePolicy 3455
このポリシーを使用すると 3455
ポリシーの詳細 3455
ポリシーのバージョン 3455
JSON ポリシードキュメント 3455
詳細はこちら 3457
AWSSystemsManagerOpsDataSyncServiceRolePolicy 3457
このポリシーを使用すると 3457
ポリシーの詳細 3457
ポリシーのバージョン 3457
JSON ポリシードキュメント 3457
詳細はこちら 3461
AWSThinkboxAssetServerPolicy 3461
このポリシーを使用すると 3461
ポリシーの詳細 3461
ポリシーのバージョン 3462
JSON ポリシードキュメント 3462
詳細はこちら 3463
AWSThinkboxAWSPortalAdminPolicy 3463
このポリシーを使用すると 3463
ポリシーの詳細 3463
ポリシーのバージョン 3463
JSON ポリシードキュメント 3464
詳細はこちら 3473
AWSThinkboxAWSPortalGatewayPolicy 3474
このポリシーを使用すると 3474
ポリシーの詳細 3474
ポリシーのバージョン 3474
JSON ポリシードキュメント 3474
詳細はこちら 3476

AWSThinkboxAWSPortalWorkerPolicy 3476
このポリシーを使用すると 3476
ポリシーの詳細 3476
ポリシーのバージョン 3477
JSON ポリシードキュメント 3477
詳細はこちら 3479
AWSThinkboxDeadlineResourceTrackerAccessPolicy 3479
このポリシーを使用すると 3479
ポリシーの詳細 3479
ポリシーのバージョン 3480
JSON ポリシードキュメント 3480
詳細はこちら 3482
AWSThinkboxDeadlineResourceTrackerAdminPolicy 3483
このポリシーを使用すると 3483
ポリシーの詳細 3483
ポリシーのバージョン 3483
JSON ポリシードキュメント 3483
詳細はこちら 3489
AWSThinkboxDeadlineSpotEventPluginAdminPolicy 3489
このポリシーを使用すると 3490
ポリシーの詳細 3490
ポリシーのバージョン 3490
JSON ポリシードキュメント 3490
詳細はこちら 3493
AWSThinkboxDeadlineSpotEventPluginWorkerPolicy 3493
このポリシーを使用すると 3493
ポリシーの詳細 3493
ポリシーのバージョン 3494
JSON ポリシードキュメント 3494
詳細はこちら 3495
AWSTransferConsoleFullAccess 3495
このポリシーを使用すると 3495
ポリシーの詳細 3496
ポリシーのバージョン 3496
JSON ポリシードキュメント 3496
詳細はこちら 3497

AWSTransferFullAccess 3497
このポリシーを使用すると 3497
ポリシーの詳細 3497
ポリシーのバージョン 3498
JSON ポリシードキュメント 3498
詳細はこちら 3499
AWSTransferLoggingAccess 3499
このポリシーを使用すると 3499
ポリシーの詳細 3499
ポリシーのバージョン 3499
JSON ポリシードキュメント 3499
詳細はこちら 3500
AWSTransferReadOnlyAccess 3500
このポリシーを使用すると 3500
ポリシーの詳細 3500
ポリシーのバージョン 3501
JSON ポリシードキュメント 3501
詳細はこちら 3501
AWSTransformApplicationDeploymentPolicy 3501
このポリシーを使用すると 3502
ポリシーの詳細 3502
ポリシーのバージョン 3502
JSON ポリシードキュメント 3502
詳細はこちら 3510
AWSTransformApplicationECSDeploymentPolicy 3510
このポリシーを使用すると 3511
ポリシーの詳細 3511
ポリシーのバージョン 3511
JSON ポリシードキュメント 3511
詳細はこちら 3519
AWSTransformCustomExecuteTransformations 3519
このポリシーを使用すると 3519
ポリシーの詳細 3519
ポリシーのバージョン 3520
JSON ポリシードキュメント 3520
詳細はこちら 3520

AWSTransformCustomFullAccess 3521
このポリシーを使用すると 3521
ポリシーの詳細 3521
ポリシーのバージョン 3521
JSON ポリシードキュメント 3521
詳細はこちら 3522
AWSTransformCustomManageTransformations 3522
このポリシーを使用すると 3522
ポリシーの詳細 3522
ポリシーのバージョン 3522
JSON ポリシードキュメント 3523
詳細はこちら 3523
AWSTrustedAdvisorPriorityFullAccess 3524
このポリシーを使用すると 3524
ポリシーの詳細 3524
ポリシーのバージョン 3524
JSON ポリシードキュメント 3524
詳細はこちら 3526
AWSTrustedAdvisorPriorityReadOnlyAccess 3526
このポリシーを使用すると 3526
ポリシーの詳細 3526
ポリシーのバージョン 3527
JSON ポリシードキュメント 3527
詳細はこちら 3528
AWSTrustedAdvisorReportingServiceRolePolicy 3528
このポリシーを使用すると 3528
ポリシーの詳細 3528
ポリシーのバージョン 3529
JSON ポリシードキュメント 3529
詳細はこちら 3529
AWSTrustedAdvisorServiceRolePolicy 3530
このポリシーを使用すると 3530
ポリシーの詳細 3530
ポリシーのバージョン 3530
JSON ポリシードキュメント 3530
詳細はこちら 3533

AWSUserAttributeCostAllocationPolicy 3533
このポリシーを使用すると 3534
ポリシーの詳細 3534
ポリシーのバージョン 3534
JSON ポリシードキュメント 3534
詳細はこちら 3534
AWSUserNotificationsServiceLinkedRolePolicy 3535
このポリシーを使用すると 3535
ポリシーの詳細 3535
ポリシーのバージョン 3535
JSON ポリシードキュメント 3535
詳細はこちら 3537
AWSVendorInsightsAssessorFullAccess 3537
このポリシーを使用すると 3537
ポリシーの詳細 3537
ポリシーのバージョン 3538
JSON ポリシードキュメント 3538
詳細はこちら 3539
AWSVendorInsightsAssessorReadOnly 3539
このポリシーを使用すると 3539
ポリシーの詳細 3539
ポリシーのバージョン 3540
JSON ポリシードキュメント 3540
詳細はこちら 3540
AWSVendorInsightsVendorFullAccess 3541
このポリシーを使用すると 3541
ポリシーの詳細 3541
ポリシーのバージョン 3541
JSON ポリシードキュメント 3541
詳細はこちら 3543
AWSVendorInsightsVendorReadOnly 3543
このポリシーを使用すると 3543
ポリシーの詳細 3543
ポリシーのバージョン 3544
JSON ポリシードキュメント 3544
詳細はこちら 3545

AWSVpcLatticeServiceRolePolicy 3545
このポリシーを使用すると 3545
ポリシーの詳細 3545
ポリシーのバージョン 3546
JSON ポリシードキュメント 3546
詳細はこちら 3548
AWSVPCS2SVpnServiceRolePolicy 3549
このポリシーを使用すると 3549
ポリシーの詳細 3549
ポリシーのバージョン 3549
JSON ポリシードキュメント 3549
詳細はこちら 3550
AWSVPCTransitGatewayServiceRolePolicy 3551
このポリシーを使用すると 3551
ポリシーの詳細 3551
ポリシーのバージョン 3551
JSON ポリシードキュメント 3551
詳細はこちら 3552
AWSVPCVerifiedAccessServiceRolePolicy 3552
このポリシーを使用すると 3552
ポリシーの詳細 3552
ポリシーのバージョン 3553
JSON ポリシードキュメント 3553
詳細はこちら 3554
AWSWAFConsoleFullAccess 3554
このポリシーを使用すると 3555
ポリシーの詳細 3555
ポリシーのバージョン 3555
JSON ポリシードキュメント 3555
詳細はこちら 3564
AWSWAFConsoleReadOnlyAccess 3564
このポリシーを使用すると 3564
ポリシーの詳細 3564
ポリシーのバージョン 3564
JSON ポリシードキュメント 3565
詳細はこちら 3571

AWSWAFFullAccess 3572
このポリシーを使用すると 3572
ポリシーの詳細 3572
ポリシーのバージョン 3572
JSON ポリシードキュメント 3572
詳細はこちら 3577
AWSWAFReadOnlyAccess 3577
このポリシーを使用すると 3577
ポリシーの詳細 3578
ポリシーのバージョン 3578
JSON ポリシードキュメント 3578
詳細はこちら 3581
AWSWellArchitectedDiscoveryServiceRolePolicy 3581
このポリシーを使用すると 3582
ポリシーの詳細 3582
ポリシーのバージョン 3582
JSON ポリシードキュメント 3582
詳細はこちら 3584
AWSWellArchitectedOrganizationsServiceRolePolicy 3584
このポリシーを使用すると 3584
ポリシーの詳細 3584
ポリシーのバージョン 3584
JSON ポリシードキュメント 3584
詳細はこちら 3585
AWSWickrFullAccess 3585
このポリシーを使用すると 3585
ポリシーの詳細 3585
ポリシーのバージョン 3586
JSON ポリシードキュメント 3586
詳細はこちら 3586
AWSXrayCrossAccountSharingConfiguration 3586
このポリシーを使用すると 3587
ポリシーの詳細 3587
ポリシーのバージョン 3587
JSON ポリシードキュメント 3587
詳細はこちら 3588

AWSXRayDaemonWriteAccess 3588
このポリシーを使用すると 3588
ポリシーの詳細 3588
ポリシーのバージョン 3589
JSON ポリシードキュメント 3589
詳細はこちら 3589
AWSXrayFullAccess 3590
このポリシーを使用すると 3590
ポリシーの詳細 3590
ポリシーのバージョン 3590
JSON ポリシードキュメント 3590
詳細はこちら 3591
AWSXrayReadOnlyAccess 3591
このポリシーを使用すると 3591
ポリシーの詳細 3591
ポリシーのバージョン 3591
JSON ポリシードキュメント 3592
詳細はこちら 3592
AWSXrayWriteOnlyAccess 3593
このポリシーを使用すると 3593
ポリシーの詳細 3593
ポリシーのバージョン 3593
JSON ポリシードキュメント 3593
詳細はこちら 3594
AWSZonalAutoshiftPracticeRunSLRPolicy 3594
このポリシーを使用すると 3594
ポリシーの詳細 3594
ポリシーのバージョン 3594
JSON ポリシードキュメント 3595
詳細はこちら 3596
AWSZoneGroupAccessManagementServiceRolePolicy 3596
このポリシーを使用すると 3596
ポリシーの詳細 3596
ポリシーのバージョン 3596
JSON ポリシードキュメント 3596
詳細はこちら 3597

BatchServiceRolePolicy 3597
このポリシーを使用すると 3597
ポリシーの詳細 3597
ポリシーのバージョン 3598
JSON ポリシードキュメント 3598
詳細はこちら 3604
BedrockAgentCoreFullAccess 3604
このポリシーを使用すると 3604
ポリシーの詳細 3604
ポリシーのバージョン 3605
JSON ポリシードキュメント 3605
詳細はこちら 3614
BedrockAgentCoreNetworkServiceRolePolicy 3614
このポリシーを使用すると 3614
ポリシーの詳細 3614
ポリシーのバージョン 3615
JSON ポリシードキュメント 3615
詳細はこちら 3617
BedrockAgentCoreRuntimeIdentityServiceRolePolicy 3617
このポリシーを使用すると 3617
ポリシーの詳細 3617
ポリシーのバージョン 3617
JSON ポリシードキュメント 3618
詳細はこちら 3618
Billing 3618
このポリシーを使用すると 3618
ポリシーの詳細 3618
ポリシーのバージョン 3619
JSON ポリシードキュメント 3619
詳細はこちら 3623
BudgetsServiceRolePolicy 3623
このポリシーを使用すると 3623
ポリシーの詳細 3623
ポリシーのバージョン 3623
JSON ポリシードキュメント 3624
詳細はこちら 3624

CertificateManagerServiceRolePolicy 3624
このポリシーを使用すると 3624
ポリシーの詳細 3624
ポリシーのバージョン 3625
JSON ポリシードキュメント 3625
詳細はこちら 3625
ClientVPNServiceConnectionsRolePolicy 3625
このポリシーを使用すると 3626
ポリシーの詳細 3626
ポリシーのバージョン 3626
JSON ポリシードキュメント 3626
詳細はこちら 3627
ClientVPNServiceRolePolicy 3627
このポリシーを使用すると 3627
ポリシーの詳細 3627
ポリシーのバージョン 3627
JSON ポリシードキュメント 3627
詳細はこちら 3628
CloudFormationStackSetsOrgAdminServiceRolePolicy 3628
このポリシーを使用すると 3629
ポリシーの詳細 3629
ポリシーのバージョン 3629
JSON ポリシードキュメント 3629
詳細はこちら 3630
CloudFormationStackSetsOrgMemberServiceRolePolicy 3630
このポリシーを使用すると 3630
ポリシーの詳細 3630
ポリシーのバージョン 3630
JSON ポリシードキュメント 3631
詳細はこちら 3631
CloudFrontFullAccess 3632
このポリシーを使用すると 3632
ポリシーの詳細 3632
ポリシーのバージョン 3632
JSON ポリシードキュメント 3632
詳細はこちら 3634

CloudFrontReadOnlyAccess 3634
このポリシーを使用すると 3635
ポリシーの詳細 3635
ポリシーのバージョン 3635
JSON ポリシードキュメント 3635
詳細はこちら 3636
CloudHSMServiceRolePolicy 3636
このポリシーを使用すると 3636
ポリシーの詳細 3636
ポリシーのバージョン 3637
JSON ポリシードキュメント 3637
詳細はこちら 3637
CloudSearchFullAccess 3637
このポリシーを使用すると 3638
ポリシーの詳細 3638
ポリシーのバージョン 3638
JSON ポリシードキュメント 3638
詳細はこちら 3638
CloudSearchReadOnlyAccess 3639
このポリシーを使用すると 3639
ポリシーの詳細 3639
ポリシーのバージョン 3639
JSON ポリシードキュメント 3639
詳細はこちら 3640
CloudTrailEventContext 3640
このポリシーを使用すると 3640
ポリシーの詳細 3640
ポリシーのバージョン 3640
JSON ポリシードキュメント 3641
詳細はこちら 3642
CloudTrailServiceRolePolicy 3643
このポリシーを使用すると 3643
ポリシーの詳細 3643
ポリシーのバージョン 3643
JSON ポリシードキュメント 3643
詳細はこちら 3645

CloudWatch-CrossAccountAccess 3645
このポリシーを使用すると 3645
ポリシーの詳細 3645
ポリシーのバージョン 3646
JSON ポリシードキュメント 3646
詳細はこちら 3646
CloudWatchActionsEC2Access 3646
このポリシーを使用すると 3646
ポリシーの詳細 3647
ポリシーのバージョン 3647
JSON ポリシードキュメント 3647
詳細はこちら 3647
CloudWatchAgentAdminPolicy 3648
このポリシーを使用すると 3648
ポリシーの詳細 3648
ポリシーのバージョン 3648
JSON ポリシードキュメント 3648
詳細はこちら 3649
CloudWatchAgentServerPolicy 3649
このポリシーを使用すると 3650
ポリシーの詳細 3650
ポリシーのバージョン 3650
JSON ポリシードキュメント 3650
詳細はこちら 3651
CloudWatchApplicationInsightsFullAccess 3651
このポリシーを使用すると 3651
ポリシーの詳細 3651
ポリシーのバージョン 3652
JSON ポリシードキュメント 3652
詳細はこちら 3653
CloudWatchApplicationInsightsReadOnlyAccess 3653
このポリシーを使用すると 3654
ポリシーの詳細 3654
ポリシーのバージョン 3654
JSON ポリシードキュメント 3654
詳細はこちら 3654

CloudwatchApplicationInsightsServiceLinkedRolePolicy 3655
このポリシーを使用すると 3655
ポリシーの詳細 3655
ポリシーのバージョン 3655
JSON ポリシードキュメント 3655
詳細はこちら 3666
CloudWatchApplicationSignalsFullAccess 3666
このポリシーを使用すると 3666
ポリシーの詳細 3666
ポリシーのバージョン 3667
JSON ポリシードキュメント 3667
詳細はこちら 3672
CloudWatchApplicationSignalsReadOnlyAccess 3672
このポリシーを使用すると 3672
ポリシーの詳細 3672
ポリシーのバージョン 3673
JSON ポリシードキュメント 3673
詳細はこちら 3677
CloudWatchApplicationSignalsServiceRolePolicy 3677
このポリシーを使用すると 3677
ポリシーの詳細 3677
ポリシーのバージョン 3678
JSON ポリシードキュメント 3678
詳細はこちら 3681
CloudWatchAutomaticDashboardsAccess 3681
このポリシーを使用すると 3681
ポリシーの詳細 3681
ポリシーのバージョン 3681
JSON ポリシードキュメント 3682
詳細はこちら 3683
CloudWatchCrossAccountSharingConfiguration 3683
このポリシーを使用すると 3683
ポリシーの詳細 3683
ポリシーのバージョン 3684
JSON ポリシードキュメント 3684
詳細はこちら 3685

CloudWatchEventsBuiltInTargetExecutionAccess 3685
このポリシーを使用すると 3685
ポリシーの詳細 3685
ポリシーのバージョン 3685
JSON ポリシードキュメント 3686
詳細はこちら 3686
CloudWatchEventsFullAccess 3686
このポリシーを使用すると 3686
ポリシーの詳細 3687
ポリシーのバージョン 3687
JSON ポリシードキュメント 3687
詳細はこちら 3689
CloudWatchEventsInvocationAccess 3689
このポリシーを使用すると 3689
ポリシーの詳細 3689
ポリシーのバージョン 3690
JSON ポリシードキュメント 3690
詳細はこちら 3690
CloudWatchEventsReadOnlyAccess 3690
このポリシーを使用すると 3691
ポリシーの詳細 3691
ポリシーのバージョン 3691
JSON ポリシードキュメント 3691
詳細はこちら 3692
CloudWatchEventsServiceRolePolicy 3693
このポリシーを使用すると 3693
ポリシーの詳細 3693
ポリシーのバージョン 3693
JSON ポリシードキュメント 3693
詳細はこちら 3694
CloudWatchFullAccess 3694
このポリシーを使用すると 3694
ポリシーの詳細 3694
ポリシーのバージョン 3694
JSON ポリシードキュメント 3695
詳細はこちら 3696

CloudWatchFullAccessV2 ... 3696
このポリシーを使用すると ... 3696
ポリシーの詳細 ... 3696
ポリシーのバージョン ... 3696
JSON ポリシードキュメント ... 3696
詳細はこちら ... 3702
CloudWatchInternetMonitorFullAccess ... 3702
このポリシーを使用すると ... 3702
ポリシーの詳細 ... 3702
ポリシーのバージョン ... 3703
JSON ポリシードキュメント ... 3703
詳細はこちら ... 3705
CloudWatchInternetMonitorReadOnlyAccess ... 3705
このポリシーを使用すると ... 3705
ポリシーの詳細 ... 3705
ポリシーのバージョン ... 3705
JSON ポリシードキュメント ... 3706
詳細はこちら ... 3706
CloudWatchInternetMonitorServiceRolePolicy ... 3707
このポリシーを使用すると ... 3707
ポリシーの詳細 ... 3707
ポリシーのバージョン ... 3707
JSON ポリシードキュメント ... 3707
詳細はこちら ... 3708
CloudWatchLambdaApplicationSignalsExecutionRolePolicy ... 3709
このポリシーを使用すると ... 3709
ポリシーの詳細 ... 3709
ポリシーのバージョン ... 3709
JSON ポリシードキュメント ... 3709
詳細はこちら ... 3710
CloudWatchLambdaInsightsExecutionRolePolicy ... 3710
このポリシーを使用すると ... 3711
ポリシーの詳細 ... 3711
ポリシーのバージョン ... 3711
JSON ポリシードキュメント ... 3711
詳細はこちら ... 3712

CloudWatchLogsCrossAccountSharingConfiguration 3712
このポリシーを使用すると 3712
ポリシーの詳細 3712
ポリシーのバージョン 3712
JSON ポリシードキュメント 3713
詳細はこちら 3713
CloudWatchLogsFullAccess 3714
このポリシーを使用すると 3714
ポリシーの詳細 3714
ポリシーのバージョン 3714
JSON ポリシードキュメント 3714
詳細はこちら 3715
CloudWatchLogsReadOnlyAccess 3715
このポリシーを使用すると 3715
ポリシーの詳細 3715
ポリシーのバージョン 3715
JSON ポリシードキュメント 3716
詳細はこちら 3716
CloudWatchNetworkFlowMonitorAgentPublishPolicy 3717
このポリシーを使用すると 3717
ポリシーの詳細 3717
ポリシーのバージョン 3717
JSON ポリシードキュメント 3717
詳細はこちら 3718
CloudWatchNetworkFlowMonitorServiceRolePolicy 3718
このポリシーを使用すると 3718
ポリシーの詳細 3718
ポリシーのバージョン 3719
JSON ポリシードキュメント 3719
詳細はこちら 3720
CloudWatchNetworkFlowMonitorTopologyServiceRolePolicy 3720
このポリシーを使用すると 3720
ポリシーの詳細 3720
ポリシーのバージョン 3720
JSON ポリシードキュメント 3721
詳細はこちら 3722

CloudWatchNetworkMonitorServiceRolePolicy 3722
このポリシーを使用すると 3722
ポリシーの詳細 3722
ポリシーのバージョン 3722
JSON ポリシードキュメント 3723
詳細はこちら 3724
CloudWatchOpenSearchDashboardAccess 3724
このポリシーを使用すると 3724
ポリシーの詳細 3724
ポリシーのバージョン 3725
JSON ポリシードキュメント 3725
詳細はこちら 3727
CloudWatchOpenSearchDashboardsFullAccess 3727
このポリシーを使用すると 3728
ポリシーの詳細 3728
ポリシーのバージョン 3728
JSON ポリシードキュメント 3728
詳細はこちら 3735
CloudWatchReadOnlyAccess 3735
このポリシーを使用すると 3735
ポリシーの詳細 3736
ポリシーのバージョン 3736
JSON ポリシードキュメント 3736
詳細はこちら 3739
CloudWatchSyntheticsFullAccess 3739
このポリシーを使用すると 3739
ポリシーの詳細 3739
ポリシーのバージョン 3739
JSON ポリシードキュメント 3740
詳細はこちら 3745
CloudWatchSyntheticsReadOnlyAccess 3745
このポリシーを使用すると 3745
ポリシーの詳細 3745
ポリシーのバージョン 3745
JSON ポリシードキュメント 3746
詳細はこちら 3746

ComprehendDataAccessRolePolicy 3746
このポリシーを使用すると 3746
ポリシーの詳細 3747
ポリシーのバージョン 3747
JSON ポリシードキュメント 3747
詳細はこちら 3747
ComprehendFullAccess 3748
このポリシーを使用すると 3748
ポリシーの詳細 3748
ポリシーのバージョン 3748
JSON ポリシードキュメント 3748
詳細はこちら 3749
ComprehendMedicalFullAccess 3749
このポリシーを使用すると 3749
ポリシーの詳細 3749
ポリシーのバージョン 3749
JSON ポリシードキュメント 3750
詳細はこちら 3750
ComprehendReadOnly 3750
このポリシーを使用すると 3750
ポリシーの詳細 3750
ポリシーのバージョン 3751
JSON ポリシードキュメント 3751
詳細はこちら 3752
ComputeOptimizerAutomationServiceRolePolicy 3752
このポリシーを使用すると 3753
ポリシーの詳細 3753
ポリシーのバージョン 3753
JSON ポリシードキュメント 3753
詳細はこちら 3755
ComputeOptimizerReadOnlyAccess 3755
このポリシーを使用すると 3755
ポリシーの詳細 3755
ポリシーのバージョン 3755
JSON ポリシードキュメント 3756
詳細はこちら 3757

ComputeOptimizerServiceRolePolicy 3757
このポリシーを使用すると 3757
ポリシーの詳細 3757
ポリシーのバージョン 3757
JSON ポリシードキュメント 3758
詳細はこちら 3759
ConfigConformsServiceRolePolicy 3759
このポリシーを使用すると 3759
ポリシーの詳細 3759
ポリシーのバージョン 3760
JSON ポリシードキュメント 3760
詳細はこちら 3763
ConsoleFullAccessFromVercel 3763
このポリシーを使用すると 3763
ポリシーの詳細 3763
ポリシーのバージョン 3763
JSON ポリシードキュメント 3763
詳細はこちら 3767
ConsoleViewOnlyAccessFromVercel 3767
このポリシーを使用すると 3768
ポリシーの詳細 3768
ポリシーのバージョン 3768
JSON ポリシードキュメント 3768
詳細はこちら 3770
CostOptimizationHubAdminAccess 3770
このポリシーを使用すると 3770
ポリシーの詳細 3770
ポリシーのバージョン 3770
JSON ポリシードキュメント 3771
詳細はこちら 3772
CostOptimizationHubReadOnlyAccess 3772
このポリシーを使用すると 3772
ポリシーの詳細 3772
ポリシーのバージョン 3773
JSON ポリシードキュメント 3773
詳細はこちら 3773

CostOptimizationHubServiceRolePolicy 3774
このポリシーを使用すると 3774
ポリシーの詳細 3774
ポリシーのバージョン 3774
JSON ポリシードキュメント 3774
詳細はこちら 3775
CustomerProfilesServiceLinkedRolePolicy 3776
このポリシーを使用すると 3776
ポリシーの詳細 3776
ポリシーのバージョン 3776
JSON ポリシードキュメント 3776
詳細はこちら 3777
DatabaseAdministrator 3778
このポリシーを使用すると 3778
ポリシーの詳細 3778
ポリシーのバージョン 3778
JSON ポリシードキュメント 3778
詳細はこちら 3781
DataScientist 3781
このポリシーを使用すると 3781
ポリシーの詳細 3781
ポリシーのバージョン 3782
JSON ポリシードキュメント 3782
詳細はこちら 3785
DAXServiceRolePolicy 3786
このポリシーを使用すると 3786
ポリシーの詳細 3786
ポリシーのバージョン 3786
JSON ポリシードキュメント 3786
詳細はこちら 3787
DeclarativePoliciesEC2Report 3787
このポリシーを使用すると 3787
ポリシーの詳細 3787
ポリシーのバージョン 3788
JSON ポリシードキュメント 3788
詳細はこちら 3788

DynamoDBCloudWatchContributorInsightsServiceRolePolicy 3789
このポリシーを使用すると 3789
ポリシーの詳細 3789
ポリシーのバージョン 3789
JSON ポリシードキュメント 3789
詳細はこちら 3790
DynamoDBGlobalTableSettingsManagementServiceRolePolicy 3790
このポリシーを使用すると 3790
ポリシーの詳細 3790
ポリシーのバージョン 3791
JSON ポリシードキュメント 3791
詳細はこちら 3792
DynamoDBKinesisReplicationServiceRolePolicy 3792
このポリシーを使用すると 3792
ポリシーの詳細 3792
ポリシーのバージョン 3793
JSON ポリシードキュメント 3793
詳細はこちら 3793
DynamoDBReplicationServiceRolePolicy 3794
このポリシーを使用すると 3794
ポリシーの詳細 3794
ポリシーのバージョン 3794
JSON ポリシードキュメント 3794
詳細はこちら 3795
EC2FastLaunchFullAccess 3796
このポリシーを使用すると 3796
ポリシーの詳細 3796
ポリシーのバージョン 3796
JSON ポリシードキュメント 3796
詳細はこちら 3803
EC2FastLaunchServiceRolePolicy 3803
このポリシーを使用すると 3804
ポリシーの詳細 3804
ポリシーのバージョン 3804
JSON ポリシードキュメント 3804
詳細はこちら 3810

EC2FleetTimeShiftableServiceRolePolicy 3810
このポリシーを使用すると 3810
ポリシーの詳細 3811
ポリシーのバージョン 3811
JSON ポリシードキュメント 3811
詳細はこちら 3812
Ec2ImageBuilderCrossAccountDistributionAccess 3813
このポリシーを使用すると 3813
ポリシーの詳細 3813
ポリシーのバージョン 3813
JSON ポリシードキュメント 3813
詳細はこちら 3814
EC2ImageBuilderLifecycleExecutionPolicy 3814
このポリシーを使用すると 3814
ポリシーの詳細 3814
ポリシーのバージョン 3815
JSON ポリシードキュメント 3815
詳細はこちら 3817
EC2InstanceConnect 3817
このポリシーを使用すると 3817
ポリシーの詳細 3817
ポリシーのバージョン 3817
JSON ポリシードキュメント 3818
詳細はこちら 3818
Ec2InstanceConnectEndpoint 3818
このポリシーを使用すると 3819
ポリシーの詳細 3819
ポリシーのバージョン 3819
JSON ポリシードキュメント 3819
詳細はこちら 3822
EC2InstanceProfileForImageBuilder 3822
このポリシーを使用すると 3822
ポリシーの詳細 3822
ポリシーのバージョン 3822
JSON ポリシードキュメント 3823
詳細はこちら 3825

EC2InstanceProfileForImageBuilderECRContainerBuilds 3825
このポリシーを使用すると 3826
ポリシーの詳細 3826
ポリシーのバージョン 3826
JSON ポリシードキュメント 3826
詳細はこちら 3827
ECRReplicationServiceRolePolicy 3828
このポリシーを使用すると 3828
ポリシーの詳細 3828
ポリシーのバージョン 3828
JSON ポリシードキュメント 3828
詳細はこちら 3829
ECRTemplateServiceRolePolicy 3829
このポリシーを使用すると 3829
ポリシーの詳細 3829
ポリシーのバージョン 3829
JSON ポリシードキュメント 3830
詳細はこちら 3830
ElastiCacheServiceRolePolicy 3830
このポリシーを使用すると 3830
ポリシーの詳細 3831
ポリシーのバージョン 3831
JSON ポリシードキュメント 3831
詳細はこちら 3833
ElasticLoadBalancingFullAccess 3833
このポリシーを使用すると 3833
ポリシーの詳細 3833
ポリシーのバージョン 3834
JSON ポリシードキュメント 3834
詳細はこちら 3835
ElasticLoadBalancingReadOnly 3835
このポリシーを使用すると 3835
ポリシーの詳細 3836
ポリシーのバージョン 3836
JSON ポリシードキュメント 3836
詳細はこちら 3837

ElementalActivationsDownloadSoftwareAccess 3837
このポリシーを使用すると 3837
ポリシーの詳細 3837
ポリシーのバージョン 3838
JSON ポリシードキュメント 3838
詳細はこちら 3838
ElementalActivationsFullAccess 3839
このポリシーを使用すると 3839
ポリシーの詳細 3839
ポリシーのバージョン 3839
JSON ポリシードキュメント 3839
詳細はこちら 3840
ElementalActivationsGenerateLicenses 3840
このポリシーを使用すると 3840
ポリシーの詳細 3840
ポリシーのバージョン 3840
JSON ポリシードキュメント 3841
詳細はこちら 3841
ElementalActivationsReadOnlyAccess 3841
このポリシーを使用すると 3841
ポリシーの詳細 3842
ポリシーのバージョン 3842
JSON ポリシードキュメント 3842
詳細はこちら 3842
ElementalAppliancesSoftwareFullAccess 3843
このポリシーを使用すると 3843
ポリシーの詳細 3843
ポリシーのバージョン 3843
JSON ポリシードキュメント 3843
詳細はこちら 3844
ElementalAppliancesSoftwareReadOnlyAccess 3844
このポリシーを使用すると 3844
ポリシーの詳細 3844
ポリシーのバージョン 3844
JSON ポリシードキュメント 3845
詳細はこちら 3845

ElementalSupportCenterFullAccess 3845
このポリシーを使用すると 3845
ポリシーの詳細 3846
ポリシーのバージョン 3846
JSON ポリシードキュメント 3846
詳細はこちら 3846
EMRDescribeClusterPolicyForEMRWAL 3847
このポリシーを使用すると 3847
ポリシーの詳細 3847
ポリシーのバージョン 3847
JSON ポリシードキュメント 3847
詳細はこちら 3848
FMSServiceRolePolicy 3848
このポリシーを使用すると 3848
ポリシーの詳細 3848
ポリシーのバージョン 3848
JSON ポリシードキュメント 3849
詳細はこちら 3865
FSxDeleteServiceLinkedRoleAccess 3865
このポリシーを使用すると 3865
ポリシーの詳細 3865
ポリシーのバージョン 3866
JSON ポリシードキュメント 3866
詳細はこちら 3866
GameLiftContainerFleetPolicy 3867
このポリシーを使用すると 3867
ポリシーの詳細 3867
ポリシーのバージョン 3867
JSON ポリシードキュメント 3867
詳細はこちら 3868
GameLiftGameServerGroupPolicy 3869
このポリシーを使用すると 3869
ポリシーの詳細 3869
ポリシーのバージョン 3869
JSON ポリシードキュメント 3869
詳細はこちら 3871

GitLabDuoWithAmazonQPermissionsPolicy 3871
このポリシーを使用すると 3871
ポリシーの詳細 3871
ポリシーのバージョン 3871
JSON ポリシードキュメント 3872
詳細はこちら 3873
GlobalAcceleratorFullAccess 3873
このポリシーを使用すると 3873
ポリシーの詳細 3873
ポリシーのバージョン 3873
JSON ポリシードキュメント 3873
詳細はこちら 3874
GlobalAcceleratorReadOnlyAccess 3875
このポリシーを使用すると 3875
ポリシーの詳細 3875
ポリシーのバージョン 3875
JSON ポリシードキュメント 3875
詳細はこちら 3876
GreengrassOTAUpdateArtifactAccess 3876
このポリシーを使用すると 3876
ポリシーの詳細 3876
ポリシーのバージョン 3876
JSON ポリシードキュメント 3877
詳細はこちら 3877
GroundTruthSyntheticConsoleFullAccess 3877
このポリシーを使用すると 3878
ポリシーの詳細 3878
ポリシーのバージョン 3878
JSON ポリシードキュメント 3878
詳細はこちら 3878
GroundTruthSyntheticConsoleReadOnlyAccess 3879
このポリシーを使用すると 3879
ポリシーの詳細 3879
ポリシーのバージョン 3879
JSON ポリシードキュメント 3879
詳細はこちら 3880

Health_OrganizationsServiceRolePolicy 3880
このポリシーを使用すると 3880
ポリシーの詳細 3880
ポリシーのバージョン 3881
JSON ポリシードキュメント 3881
詳細はこちら 3881
IAMAccessAdvisorReadOnly 3881
このポリシーを使用すると 3882
ポリシーの詳細 3882
ポリシーのバージョン 3882
JSON ポリシードキュメント 3882
詳細はこちら 3883
IAMAccessAnalyzerFullAccess 3883
このポリシーを使用すると 3883
ポリシーの詳細 3883
ポリシーのバージョン 3884
JSON ポリシードキュメント 3884
詳細はこちら 3885
IAMAccessAnalyzerReadOnlyAccess 3885
このポリシーを使用すると 3885
ポリシーの詳細 3885
ポリシーのバージョン 3885
JSON ポリシードキュメント 3886
詳細はこちら 3886
IAMFullAccess 3886
このポリシーを使用すると 3887
ポリシーの詳細 3887
ポリシーのバージョン 3887
JSON ポリシードキュメント 3887
詳細はこちら 3888
IAMReadOnlyAccess 3888
このポリシーを使用すると 3888
ポリシーの詳細 3888
ポリシーのバージョン 3888
JSON ポリシードキュメント 3889
詳細はこちら 3889

IAMSelfManageServiceSpecificCredentials 3889
このポリシーを使用すると 3889
ポリシーの詳細 3890
ポリシーのバージョン 3890
JSON ポリシードキュメント 3890
詳細はこちら 3890
IAMUserChangePassword 3891
このポリシーを使用すると 3891
ポリシーの詳細 3891
ポリシーのバージョン 3891
JSON ポリシードキュメント 3891
詳細はこちら 3892
IAMUserSSHKeys 3892
このポリシーを使用すると 3892
ポリシーの詳細 3892
ポリシーのバージョン 3893
JSON ポリシードキュメント 3893
詳細はこちら 3893
IVSFullAccess 3893
このポリシーを使用すると 3894
ポリシーの詳細 3894
ポリシーのバージョン 3894
JSON ポリシードキュメント 3894
詳細はこちら 3895
IVSReadOnlyAccess 3895
このポリシーを使用すると 3895
ポリシーの詳細 3895
ポリシーのバージョン 3895
JSON ポリシードキュメント 3895
詳細はこちら 3897
IVSRecordToS3 3897
このポリシーを使用すると 3897
ポリシーの詳細 3897
ポリシーのバージョン 3897
JSON ポリシードキュメント 3897
詳細はこちら 3898

KafkaConnectServiceRolePolicy 3898
このポリシーを使用すると 3898
ポリシーの詳細 3898
ポリシーのバージョン 3899
JSON ポリシードキュメント 3899
詳細はこちら 3900
KafkaServiceRolePolicy 3900
このポリシーを使用すると 3901
ポリシーの詳細 3901
ポリシーのバージョン 3901
JSON ポリシードキュメント 3901
詳細はこちら 3903
KeyspacesCDCServiceRolePolicy 3903
このポリシーを使用すると 3903
ポリシーの詳細 3903
ポリシーのバージョン 3904
JSON ポリシードキュメント 3904
詳細はこちら 3904
KeyspacesReplicationServiceRolePolicy 3904
このポリシーを使用すると 3905
ポリシーの詳細 3905
ポリシーのバージョン 3905
JSON ポリシードキュメント 3905
詳細はこちら 3906
LakeFormationDataAccessServiceRolePolicy 3907
このポリシーを使用すると 3907
ポリシーの詳細 3907
ポリシーのバージョン 3907
JSON ポリシードキュメント 3907
詳細はこちら 3908
LexBotPolicy 3908
このポリシーを使用すると 3908
ポリシーの詳細 3908
ポリシーのバージョン 3908
JSON ポリシードキュメント 3909
詳細はこちら 3909

LexChannelPolicy 3909
このポリシーを使用すると 3910
ポリシーの詳細 3910
ポリシーのバージョン 3910
JSON ポリシードキュメント 3910
詳細はこちら 3910
LightsailExportAccess 3911
このポリシーを使用すると 3911
ポリシーの詳細 3911
ポリシーのバージョン 3911
JSON ポリシードキュメント 3911
詳細はこちら 3912
MediaConnectGatewayInstanceRolePolicy 3912
このポリシーを使用すると 3912
ポリシーの詳細 3913
ポリシーのバージョン 3913
JSON ポリシードキュメント 3913
詳細はこちら 3913
MediaPackageServiceRolePolicy 3914
このポリシーを使用すると 3914
ポリシーの詳細 3914
ポリシーのバージョン 3914
JSON ポリシードキュメント 3914
詳細はこちら 3915
MemoryDBServiceRolePolicy 3915
このポリシーを使用すると 3915
ポリシーの詳細 3915
ポリシーのバージョン 3916
JSON ポリシードキュメント 3916
詳細はこちら 3918
MigrationHubDMSAccessServiceRolePolicy 3918
このポリシーを使用すると 3918
ポリシーの詳細 3918
ポリシーのバージョン 3919
JSON ポリシードキュメント 3919
詳細はこちら 3920

MigrationHubServiceRolePolicy 3920
このポリシーを使用すると 3920
ポリシーの詳細 3920
ポリシーのバージョン 3920
JSON ポリシードキュメント 3921
詳細はこちら 3922
MigrationHubSMSAccessServiceRolePolicy 3922
このポリシーを使用すると 3922
ポリシーの詳細 3922
ポリシーのバージョン 3923
JSON ポリシードキュメント 3923
詳細はこちら 3924
MonitronServiceRolePolicy 3924
このポリシーを使用すると 3924
ポリシーの詳細 3924
ポリシーのバージョン 3924
JSON ポリシードキュメント 3925
詳細はこちら 3925
MultiPartyApprovalFullAccess 3925
このポリシーを使用すると 3925
ポリシーの詳細 3925
ポリシーのバージョン 3926
JSON ポリシードキュメント 3926
詳細はこちら 3928
MultiPartyApprovalReadOnlyAccess 3928
このポリシーを使用すると 3929
ポリシーの詳細 3929
ポリシーのバージョン 3929
JSON ポリシードキュメント 3929
詳細はこちら 3931
NeptuneConsoleFullAccess 3931
このポリシーを使用すると 3931
ポリシーの詳細 3931
ポリシーのバージョン 3932
JSON ポリシードキュメント 3932
詳細はこちら 3937

NeptuneFullAccess 3937
このポリシーを使用すると 3938
ポリシーの詳細 3938
ポリシーのバージョン 3938
JSON ポリシードキュメント 3938
詳細はこちら 3942
NeptuneGraphReadOnlyAccess 3942
このポリシーを使用すると 3942
ポリシーの詳細 3943
ポリシーのバージョン 3943
JSON ポリシードキュメント 3943
詳細はこちら 3944
NeptuneReadOnlyAccess 3945
このポリシーを使用すると 3945
ポリシーの詳細 3945
ポリシーのバージョン 3945
JSON ポリシードキュメント 3945
詳細はこちら 3947
NetworkAdministrator 3948
このポリシーを使用すると 3948
ポリシーの詳細 3948
ポリシーのバージョン 3948
JSON ポリシードキュメント 3948
詳細はこちら 3955
NetworkSecurityDirectorServiceLinkedRolePolicy 3955
このポリシーを使用すると 3956
ポリシーの詳細 3956
ポリシーのバージョン 3956
JSON ポリシードキュメント 3956
詳細はこちら 3961
NovaActServiceRolePolicy 3962
このポリシーを使用すると 3962
ポリシーの詳細 3962
ポリシーのバージョン 3962
JSON ポリシードキュメント 3962
詳細はこちら 3963

OAMFullAccess 3963
このポリシーを使用すると 3963
ポリシーの詳細 3963
ポリシーのバージョン 3963
JSON ポリシードキュメント 3964
詳細はこちら 3964
OAMReadOnlyAccess 3964
このポリシーを使用すると 3964
ポリシーの詳細 3964
ポリシーのバージョン 3965
JSON ポリシードキュメント 3965
詳細はこちら 3965
OpensearchIngestionSelfManagedVpcePolicy 3965
このポリシーを使用すると 3966
ポリシーの詳細 3966
ポリシーのバージョン 3966
JSON ポリシードキュメント 3966
詳細はこちら 3967
PartnerCentralAccountManagementUserRoleAssociation 3967
このポリシーを使用すると 3967
ポリシーの詳細 3967
ポリシーのバージョン 3968
JSON ポリシードキュメント 3968
詳細はこちら 3969
PowerUserAccess 3969
このポリシーを使用すると 3969
ポリシーの詳細 3969
ポリシーのバージョン 3969
JSON ポリシードキュメント 3969
詳細はこちら 3970
QAppsServiceRolePolicy 3970
このポリシーを使用すると 3971
ポリシーの詳細 3971
ポリシーのバージョン 3971
JSON ポリシードキュメント 3971
詳細はこちら 3972

QBusinessQuicksightPluginPolicy 3972
このポリシーを使用すると 3972
ポリシーの詳細 3972
ポリシーのバージョン 3972
JSON ポリシードキュメント 3972
詳細はこちら 3973
QBusinessServiceRolePolicy 3973
このポリシーを使用すると 3973
ポリシーの詳細 3973
ポリシーのバージョン 3974
JSON ポリシードキュメント 3974
詳細はこちら 3975
QuickSightAccessForS3StorageManagementAnalyticsReadOnly 3976
このポリシーを使用すると 3976
ポリシーの詳細 3976
ポリシーのバージョン 3976
JSON ポリシードキュメント 3976
詳細はこちら 3977
RDSCloudHsmAuthorizationRole 3977
このポリシーを使用すると 3977
ポリシーの詳細 3977
ポリシーのバージョン 3978
JSON ポリシードキュメント 3978
詳細はこちら 3978
ReadOnlyAccess 3978
このポリシーを使用すると 3979
ポリシーの詳細 3979
ポリシーのバージョン 3979
JSON ポリシードキュメント 3979
詳細はこちら 4039
ResourceGroupsandTagEditorFullAccess 4039
このポリシーを使用すると 4040
ポリシーの詳細 4040
ポリシーのバージョン 4040
JSON ポリシードキュメント 4040
詳細はこちら 4041

ResourceGroupsandTagEditorReadOnlyAccess 4041
このポリシーを使用すると 4041
ポリシーの詳細 4041
ポリシーのバージョン 4041
JSON ポリシードキュメント 4042
詳細はこちら 4042
ResourceGroupsServiceRolePolicy 4042
このポリシーを使用すると 4043
ポリシーの詳細 4043
ポリシーのバージョン 4043
JSON ポリシードキュメント 4043
詳細はこちら 4044
ResourceGroupsTaggingAPITagUntagSupportedResources 4044
このポリシーを使用すると 4044
ポリシーの詳細 4044
ポリシーのバージョン 4044
JSON ポリシードキュメント 4045
詳細はこちら 4053
ROSAAmazonEBSCSIDriverOperatorPolicy 4053
このポリシーを使用すると 4053
ポリシーの詳細 4053
ポリシーのバージョン 4054
JSON ポリシードキュメント 4054
詳細はこちら 4057
ROSACloudNetworkConfigOperatorPolicy 4057
このポリシーを使用すると 4057
ポリシーの詳細 4058
ポリシーのバージョン 4058
JSON ポリシードキュメント 4058
詳細はこちら 4059
ROSAControlPlaneOperatorPolicy 4059
このポリシーを使用すると 4059
ポリシーの詳細 4059
ポリシーのバージョン 4060
JSON ポリシードキュメント 4060
詳細はこちら 4064

ROSAImageRegistryOperatorPolicy 4064
このポリシーを使用すると 4065
ポリシーの詳細 4065
ポリシーのバージョン 4065
JSON ポリシードキュメント 4065
詳細はこちら 4066
ROSAIngressOperatorPolicy 4067
このポリシーを使用すると 4067
ポリシーの詳細 4067
ポリシーのバージョン 4067
JSON ポリシードキュメント 4067
詳細はこちら 4068
ROSAInstallerPolicy 4068
このポリシーを使用すると 4068
ポリシーの詳細 4069
ポリシーのバージョン 4069
JSON ポリシードキュメント 4069
詳細はこちら 4077
ROSAKMSProviderPolicy 4078
このポリシーを使用すると 4078
ポリシーの詳細 4078
ポリシーのバージョン 4078
JSON ポリシードキュメント 4078
詳細はこちら 4079
ROSAKubeControllerPolicy 4079
このポリシーを使用すると 4079
ポリシーの詳細 4079
ポリシーのバージョン 4080
JSON ポリシードキュメント 4080
詳細はこちら 4084
ROSAManageSubscription 4084
このポリシーを使用すると 4084
ポリシーの詳細 4085
ポリシーのバージョン 4085
JSON ポリシードキュメント 4085
詳細はこちら 4086

ROSANodePoolManagementPolicy 4086
このポリシーを使用すると 4086
ポリシーの詳細 4086
ポリシーのバージョン 4086
JSON ポリシードキュメント 4087
詳細はこちら 4093
ROSASharedVPCEndpointPolicy 4093
このポリシーを使用すると 4093
ポリシーの詳細 4093
ポリシーのバージョン 4093
JSON ポリシードキュメント 4094
詳細はこちら 4097
ROSASharedVPCRoute53Policy 4098
このポリシーを使用すると 4098
ポリシーの詳細 4098
ポリシーのバージョン 4098
JSON ポリシードキュメント 4098
詳細はこちら 4099
ROSASRESupportPolicy 4100
このポリシーを使用すると 4100
ポリシーの詳細 4100
ポリシーのバージョン 4100
JSON ポリシードキュメント 4100
詳細はこちら 4105
ROSAWorkerInstancePolicy 4105
このポリシーを使用すると 4105
ポリシーの詳細 4105
ポリシーのバージョン 4106
JSON ポリシードキュメント 4106
詳細はこちら 4107
Route53RecoveryReadinessServiceRolePolicy 4107
このポリシーを使用すると 4107
ポリシーの詳細 4107
ポリシーのバージョン 4108
JSON ポリシードキュメント 4108
詳細はこちら 4111

Route53ResolverServiceRolePolicy 4112
このポリシーを使用すると 4112
ポリシーの詳細 4112
ポリシーのバージョン 4112
JSON ポリシードキュメント 4112
詳細はこちら 4113
RTBFabricServiceRolePolicy 4113
このポリシーを使用すると 4113
ポリシーの詳細 4113
ポリシーのバージョン 4114
JSON ポリシードキュメント 4114
詳細はこちら 4116
S3StorageLensServiceRolePolicy 4116
このポリシーを使用すると 4116
ポリシーの詳細 4116
ポリシーのバージョン 4117
JSON ポリシードキュメント 4117
詳細はこちら 4117
SageMakerStudioAdminIAMConsolePolicy 4117
このポリシーを使用すると 4118
ポリシーの詳細 4118
ポリシーのバージョン 4118
JSON ポリシードキュメント 4118
詳細はこちら 4129
SageMakerStudioAdminIAMDefaultExecutionPolicy 4129
このポリシーを使用すると 4129
ポリシーの詳細 4129
ポリシーのバージョン 4130
JSON ポリシードキュメント 4130
詳細はこちら 4151
SageMakerStudioAdminIAMPermissiveExecutionPolicy 4151
このポリシーを使用すると 4151
ポリシーの詳細 4151
ポリシーのバージョン 4151
JSON ポリシードキュメント 4152
詳細はこちら 4167

SageMakerStudioAdminProjectUserRolePolicy 4168
このポリシーを使用すると 4168
ポリシーの詳細 4168
ポリシーのバージョン 4168
JSON ポリシードキュメント 4168
詳細はこちら 4171
SageMakerStudioBedrockAgentServiceRolePolicy 4171
このポリシーを使用すると 4171
ポリシーの詳細 4171
ポリシーのバージョン 4171
JSON ポリシードキュメント 4172
詳細はこちら 4175
SageMakerStudioBedrockChatAgentUserRolePolicy 4175
このポリシーを使用すると 4175
ポリシーの詳細 4175
ポリシーのバージョン 4176
JSON ポリシードキュメント 4176
詳細はこちら 4180
SageMakerStudioBedrockEvaluationJobServiceRolePolicy 4180
このポリシーを使用すると 4180
ポリシーの詳細 4181
ポリシーのバージョン 4181
JSON ポリシードキュメント 4181
詳細はこちら 4184
SageMakerStudioBedrockFlowServiceRolePolicy 4185
このポリシーを使用すると 4185
ポリシーの詳細 4185
ポリシーのバージョン 4185
JSON ポリシードキュメント 4185
詳細はこちら 4189
SageMakerStudioBedrockFunctionExecutionRolePolicy 4189
このポリシーを使用すると 4190
ポリシーの詳細 4190
ポリシーのバージョン 4190
JSON ポリシードキュメント 4190
詳細はこちら 4191

SageMakerStudioBedrockKnowledgeBaseCustomResourcePolicy 4191
このポリシーを使用すると 4191
ポリシーの詳細 4192
ポリシーのバージョン 4192
JSON ポリシードキュメント 4192
詳細はこちら 4193
SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy 4193
このポリシーを使用すると 4193
ポリシーの詳細 4193
ポリシーのバージョン 4194
JSON ポリシードキュメント 4194
詳細はこちら 4199
SageMakerStudioBedrockPromptUserRolePolicy 4200
このポリシーを使用すると 4200
ポリシーの詳細 4200
ポリシーのバージョン 4200
JSON ポリシードキュメント 4200
詳細はこちら 4203
SageMakerStudioDomainExecutionRolePolicy 4203
このポリシーを使用すると 4203
ポリシーの詳細 4203
ポリシーのバージョン 4203
JSON ポリシードキュメント 4204
詳細はこちら 4210
SageMakerStudioDomainServiceRolePolicy 4210
このポリシーを使用すると 4210
ポリシーの詳細 4210
ポリシーのバージョン 4210
JSON ポリシードキュメント 4211
詳細はこちら 4212
SageMakerStudioEMRContainersSystemNamespaceRolePolicy 4212
このポリシーを使用すると 4212
ポリシーの詳細 4212
ポリシーのバージョン 4212
JSON ポリシードキュメント 4213
詳細はこちら 4214

SageMakerStudioEMRInstanceRolePolicy 4214
このポリシーを使用すると 4215
ポリシーの詳細 4215
ポリシーのバージョン 4215
JSON ポリシードキュメント 4215
詳細はこちら 4218
SageMakerStudioEMRServiceRolePolicy 4219
このポリシーを使用すると 4219
ポリシーの詳細 4219
ポリシーのバージョン 4219
JSON ポリシードキュメント 4219
詳細はこちら 4222
SageMakerStudioFullAccess 4222
このポリシーを使用すると 4222
ポリシーの詳細 4222
ポリシーのバージョン 4222
JSON ポリシードキュメント 4223
詳細はこちら 4233
SageMakerStudioProjectProvisioningRolePolicy 4233
このポリシーを使用すると 4233
ポリシーの詳細 4233
ポリシーのバージョン 4233
JSON ポリシードキュメント 4234
詳細はこちら 4304
SageMakerStudioProjectRoleMachineLearningPolicy 4304
このポリシーを使用すると 4304
ポリシーの詳細 4305
ポリシーのバージョン 4305
JSON ポリシードキュメント 4305
詳細はこちら 4331
SageMakerStudioProjectUserRolePermissionsBoundary 4331
このポリシーを使用すると 4331
ポリシーの詳細 4331
ポリシーのバージョン 4332
JSON ポリシードキュメント 4332
詳細はこちら 4387

SageMakerStudioProjectUserRolePolicy 4387
このポリシーを使用すると 4387
ポリシーの詳細 4388
ポリシーのバージョン 4388
JSON ポリシードキュメント 4388
詳細はこちら 4453
SageMakerStudioQueryExecutionRolePolicy 4453
このポリシーを使用すると 4453
ポリシーの詳細 4454
ポリシーのバージョン 4454
JSON ポリシードキュメント 4454
詳細はこちら 4456
SageMakerStudioUserIAMConsolePolicy 4456
このポリシーを使用すると 4456
ポリシーの詳細 4456
ポリシーのバージョン 4456
JSON ポリシードキュメント 4457
詳細はこちら 4458
SageMakerStudioUserIAMDefaultExecutionPolicy 4458
このポリシーを使用すると 4459
ポリシーの詳細 4459
ポリシーのバージョン 4459
JSON ポリシードキュメント 4459
詳細はこちら 4481
SageMakerStudioUserIAMPermissiveExecutionPolicy 4481
このポリシーを使用すると 4481
ポリシーの詳細 4481
ポリシーのバージョン 4481
JSON ポリシードキュメント 4482
詳細はこちら 4496
SecretsManagerReadWrite 4496
このポリシーを使用すると 4496
ポリシーの詳細 4496
ポリシーのバージョン 4496
JSON ポリシードキュメント 4497
詳細はこちら 4498

SecurityAgentWebAppAPIPolicy 4498
このポリシーを使用すると 4499
ポリシーの詳細 4499
ポリシーのバージョン 4499
JSON ポリシードキュメント 4499
詳細はこちら 4501
SecurityAudit 4501
このポリシーを使用すると 4501
ポリシーの詳細 4501
ポリシーのバージョン 4501
JSON ポリシードキュメント 4502
詳細はこちら 4523
SecurityLakeResourceManagementServiceRolePolicy 4524
このポリシーを使用すると 4524
ポリシーの詳細 4524
ポリシーのバージョン 4524
JSON ポリシードキュメント 4524
詳細はこちら 4530
SecurityLakeServiceLinkedRole 4530
このポリシーを使用すると 4530
ポリシーの詳細 4530
ポリシーのバージョン 4530
JSON ポリシードキュメント 4531
詳細はこちら 4533
ServerMigration_ServiceRole 4534
このポリシーを使用すると 4534
ポリシーの詳細 4534
ポリシーのバージョン 4534
JSON ポリシードキュメント 4534
詳細はこちら 4539
ServerMigrationConnector 4539
このポリシーを使用すると 4539
ポリシーの詳細 4540
ポリシーのバージョン 4540
JSON ポリシードキュメント 4540
詳細はこちら 4541

ServerMigrationServiceConsoleFullAccess 4542
このポリシーを使用すると 4542
ポリシーの詳細 4542
ポリシーのバージョン 4542
JSON ポリシードキュメント 4542
詳細はこちら 4544
ServerMigrationServiceLaunchRole 4544
このポリシーを使用すると 4544
ポリシーの詳細 4544
ポリシーのバージョン 4545
JSON ポリシードキュメント 4545
詳細はこちら 4548
ServerMigrationServiceRoleForInstanceValidation 4548
このポリシーを使用すると 4548
ポリシーの詳細 4548
ポリシーのバージョン 4548
JSON ポリシードキュメント 4549
詳細はこちら 4549
ServiceQuotasFullAccess 4549
このポリシーを使用すると 4549
ポリシーの詳細 4549
ポリシーのバージョン 4550
JSON ポリシードキュメント 4550
詳細はこちら 4551
ServiceQuotasReadOnlyAccess 4552
このポリシーを使用すると 4552
ポリシーの詳細 4552
ポリシーのバージョン 4552
JSON ポリシードキュメント 4552
詳細はこちら 4554
ServiceQuotasServiceRolePolicy 4554
このポリシーを使用すると 4554
ポリシーの詳細 4554
ポリシーのバージョン 4554
JSON ポリシードキュメント 4555
詳細はこちら 4555

SignInLocalDevelopmentAccess 4555
このポリシーを使用すると 4555
ポリシーの詳細 4555
ポリシーのバージョン 4556
JSON ポリシードキュメント 4556
詳細はこちら 4556
SimpleWorkflowFullAccess 4556
このポリシーを使用すると 4557
ポリシーの詳細 4557
ポリシーのバージョン 4557
JSON ポリシードキュメント 4557
詳細はこちら 4557
SMSVoiceServiceRolePolicy 4558
このポリシーを使用すると 4558
ポリシーの詳細 4558
ポリシーのバージョン 4558
JSON ポリシードキュメント 4558
詳細はこちら 4559
SplitCostAllocationDataServiceRolePolicy 4559
このポリシーを使用すると 4559
ポリシーの詳細 4559
ポリシーのバージョン 4560
JSON ポリシードキュメント 4560
詳細はこちら 4560
SSMQuickSetupRolePolicy 4561
このポリシーを使用すると 4561
ポリシーの詳細 4561
ポリシーのバージョン 4561
JSON ポリシードキュメント 4561
詳細はこちら 4564
SupportUser 4564
このポリシーを使用すると 4565
ポリシーの詳細 4565
ポリシーのバージョン 4565
JSON ポリシードキュメント 4565
詳細はこちら 4570

SystemAdministrator 4570
このポリシーを使用すると 4571
ポリシーの詳細 4571
ポリシーのバージョン 4571
JSON ポリシードキュメント 4571
詳細はこちら 4577
TranslateFullAccess 4577
このポリシーを使用すると 4578
ポリシーの詳細 4578
ポリシーのバージョン 4578
JSON ポリシードキュメント 4578
詳細はこちら 4579
TranslateReadOnly 4579
このポリシーを使用すると 4579
ポリシーの詳細 4579
ポリシーのバージョン 4579
JSON ポリシードキュメント 4580
詳細はこちら 4580
ViewOnlyAccess 4580
このポリシーを使用すると 4581
ポリシーの詳細 4581
ポリシーのバージョン 4581
JSON ポリシードキュメント 4581
詳細はこちら 4590
VMImportExportRoleForAWSConnector 4590
このポリシーを使用すると 4591
ポリシーの詳細 4591
ポリシーのバージョン 4591
JSON ポリシードキュメント 4591
詳細はこちら 4592
VPCLatticeFullAccess 4592
このポリシーを使用すると 4592
ポリシーの詳細 4592
ポリシーのバージョン 4593
JSON ポリシードキュメント 4593
詳細はこちら 4595

VPCLatticeReadOnlyAccess 4595
このポリシーを使用すると 4595
ポリシーの詳細 4595
ポリシーのバージョン 4595
JSON ポリシードキュメント 4596
詳細はこちら 4596
VPCLatticeServicesInvokeAccess 4597
このポリシーを使用すると 4597
ポリシーの詳細 4597
ポリシーのバージョン 4597
JSON ポリシードキュメント 4597
詳細はこちら 4598
WAFLoggingServiceRolePolicy 4598
このポリシーを使用すると 4598
ポリシーの詳細 4598
ポリシーのバージョン 4598
JSON ポリシードキュメント 4599
詳細はこちら 4599
WAFRegionalLoggingServiceRolePolicy 4599
このポリシーを使用すると 4599
ポリシーの詳細 4599
ポリシーのバージョン 4600
JSON ポリシードキュメント 4600
詳細はこちら 4600
WAFV2LoggingServiceRolePolicy 4600
このポリシーを使用すると 4601
ポリシーの詳細 4601
ポリシーのバージョン 4601
JSON ポリシードキュメント 4601
詳細はこちら 4602
WellArchitectedConsoleFullAccess 4602
このポリシーを使用すると 4602
ポリシーの詳細 4602
ポリシーのバージョン 4602
JSON ポリシードキュメント 4603
詳細はこちら 4603

WellArchitectedConsoleReadOnlyAccess 4603
このポリシーを使用すると 4603
ポリシーの詳細 4604
ポリシーのバージョン 4604
JSON ポリシードキュメント 4604
詳細はこちら 4604
WorkLinkServiceRolePolicy 4605
このポリシーを使用すると 4605
ポリシーの詳細 4605
ポリシーのバージョン 4605
JSON ポリシードキュメント 4605
詳細はこちら 4606
..... mmmmdcvii

AWS マネージドポリシーとは何ですか?

AWS マネージドポリシーは、AWS が作成および管理するスタンドアロンポリシーです。AWS マネージドポリシーは、多くの一般的なユースケースでアクセス許可を提供できるように設計されています。これにより、自身でポリシーを記述するよりも簡単に、ユーザー、グループ、ロールに許可を割り当てることができます。

AWS マネージドポリシーは、すべての AWS のユーザーが使用できるため、特定のユースケースに対して最小特権のアクセス許可が付与されない場合があることに留意してください。ユースケース別にカスタマーマネージドポリシーを定義することで、アクセス許可を絞り込むことをお勧めします。

AWS マネージドポリシーで定義したアクセス権限は変更できません。AWS が AWS マネージドポリシーに定義されているアクセス許可を更新すると、更新はポリシーがアタッチされているすべてのプリンシパルアイデンティティ (ユーザー、グループ、役割) に影響します。新しい AWS サービスを起動するか、既存のサービスで新しい API オペレーションが使用可能になると、AWS が AWS マネージドポリシーを更新する可能性が最も高くなります。

詳細については、「IAM ユーザーガイド」の「AWS マネージドポリシー」を参照してください。

ポリシーリファレンスページについて

各ポリシーリファレンスページには、以下の情報が含まれています。

- このポリシーを使用すると — ユーザー、グループ、ロールにポリシーをアタッチできるかどうか
- ポリシーの詳細
  - タイプ — AWS マネージドポリシーのタイプ
    - `AWS managed policy` — 標準 AWS マネージドポリシー
    - `Job function policy` — 一般的な業界職務に沿ったポリシー
    - `Service-linked role policy` — ユーザーに代わって the section called “AmazonRDSPreviewServiceRolePolicy” のようなアクションを実行することをサービスに許可する、サービスリンクロールにアタッチするポリシー
    - `Service role policy` — the section called “AWSControlTowerServiceRolePolicy” のようなサービスロールと連携するように設計されたポリシー
  - 作成日時 — ポリシーが最初に作成された日時
  - 編集日時 — このバージョンのポリシーが編集された日時

  - ARN — ポリシーの Amazon リソースネーム
- ポリシーのバージョン — ポリシーによって付与された許可バージョン
- JSON ポリシードキュメント — ポリシー JSON
- 詳細 — AWS マネージドポリシーに関連するドキュメントへのリンク

非推奨の AWS マネージドポリシー

AWS は、AWS マネージドポリシーを定期的に更新します。ほとんどの場合、アクセス許可をポリシーに追加します。これは、新しいサービスや機能をリリースしたときに行われます。AWS マネージドポリシーのセキュリティを向上させるために、ポリシーの範囲を縮小することがあります。ポリシーからアクセス許可を削除すると、ポリシーを非推奨の状態に設定し、新しいポリシーを利用できるようにします。AWS がサービスまたは機能を廃止すると、その機能の AWS マネージドポリシーも廃止されます。

使用しているポリシーが廃止されたというメール通知を受け取った場合は、直ちに対応することをお勧めします。ポリシーの変更を特定し、ワークフローを更新してください。AWS が交換ポリシーを提供する場合、影響を受けるすべてのアイデンティティ (ユーザー、グループ、およびロール) にそのポリシーをアタッチした後、それらのアイデンティティから廃止されたポリシーをデタッチします。

非推奨のポリシーには以下のような特徴があります。

- このガイドからは削除されています。
- アクセス許可は、現在アタッチされているすべてのアイデンティティに対して引き続き機能します。
- ポリシーがアイデンティティにアタッチされているアカウントでは、IAM コンソールの [Policies] リストに警告アイコンと共に表示されます。
- 新しいアイデンティティにはアタッチできません。現在のアイデンティティからポリシーをデタッチした場合、再アタッチすることはできません。
- 現在のすべての工ンティティからポリシーをデタッチしたら、そのポリシーは表示されなくなります。

AWS マネージドポリシー

AWS マネージドポリシー

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

- AmazonAppStreamServiceAccess
- AmazonAthenaFullAccess
- AmazonAthenaServiceRolePolicy
- AmazonAugmentedAIFullAccess
- AmazonAugmentedAIHumanLoopFullAccess
- AmazonAugmentedAIIntegratedAPIAccess
- AmazonAuroraDSQLConsoleFullAccess
- AmazonAuroraDSQLFullAccess
- AmazonAuroraDSQLReadOnlyAccess
- AmazonBedrockAgentCoreMemoryBedrockModelInferenceExecutionRolePolicy
- AmazonBedrockFullAccess
- AmazonBedrockLimitedAccess
- AmazonBedrockMantleFullAccess
- AmazonBedrockMantleInferenceAccess
- AmazonBedrockMantleReadOnly
- AmazonBedrockMarketplaceAccess
- AmazonBedrockReadOnly
- AmazonBedrockStudioPermissionsBoundary
- AmazonBraketFullAccess
- AmazonBraketJobsExecutionPolicy
- AmazonBraketServiceRolePolicy
- AmazonChimeFullAccess
- AmazonChimeReadOnly
- AmazonChimeSDK
- AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy
- AmazonChimeSDKMessagingServiceRolePolicy
- AmazonChimeServiceRolePolicy
- AmazonChimeTranscriptionServiceLinkedRolePolicy
- AmazonChimeUserManagement

- AmazonChimeVoiceConnectorServiceLinkedRolePolicy
- AmazonCloudDirectoryFullAccess
- AmazonCloudDirectoryReadOnlyAccess
- AmazonCloudWatchEvidentlyFullAccess
- AmazonCloudWatchEvidentlyReadOnlyAccess
- AmazonCloudWatchEvidentlyServiceRolePolicy
- AmazonCloudWatchRUMFullAccess
- AmazonCloudWatchRUMReadOnlyAccess
- AmazonCloudWatchRUMServiceRolePolicy
- AmazonCodeCatalystFullAccess
- AmazonCodeCatalystReadOnlyAccess
- AmazonCodeCatalystSupportAccess
- AmazonCodeGuruProfilerAgentAccess
- AmazonCodeGuruProfilerFullAccess
- AmazonCodeGuruProfilerReadOnlyAccess
- AmazonCodeGuruReviewerFullAccess
- AmazonCodeGuruReviewerReadOnlyAccess
- AmazonCodeGuruReviewerServiceRolePolicy
- AmazonCodeGuruSecurityFullAccess
- AmazonCodeGuruSecurityScanAccess
- AmazonCognitoDeveloperAuthenticatedIdentities
- AmazonCognitoIdpEmailServiceRolePolicy
- AmazonCognitoIdpServiceRolePolicy
- AmazonCognitoPowerUser
- AmazonCognitoReadOnly
- AmazonCognitoUnAuthedIdentitiesSessionPolicy
- AmazonCognitoUnauthenticatedIdentities
- AmazonConnect_FullAccess
- AmazonConnectCampaignsServiceLinkedRolePolicy

- AmazonConnectReadOnlyAccess
- AmazonConnectServiceLinkedRolePolicy
- AmazonConnectSynchronizationServiceRolePolicy
- AmazonConnectVoiceIDFullAccess
- AmazonDataZoneBedrockModelConsumptionPolicy
- AmazonDataZoneBedrockModelManagementPolicy
- AmazonDataZoneDomainExecutionRolePolicy
- AmazonDataZoneEnvironmentRolePermissionsBoundary
- AmazonDataZoneFullAccess
- AmazonDataZoneFullUserAccess
- AmazonDataZoneGlueManageAccessRolePolicy
- AmazonDataZonePortalFullAccessPolicy
- AmazonDataZonePreviewConsoleFullAccess
- AmazonDataZoneProjectDeploymentPermissionsBoundary
- AmazonDataZoneProjectRolePermissionsBoundary
- AmazonDataZoneRedshiftGlueProvisioningPolicy
- AmazonDataZoneRedshiftManageAccessRolePolicy
- AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary
- AmazonDataZoneSageMakerManageAccessRolePolicy
- AmazonDataZoneSageMakerProvisioningRolePolicy
- AmazonDetectiveFullAccess
- AmazonDetectiveInvestigatorAccess
- AmazonDetectiveMemberAccess
- AmazonDetectiveOrganizationsAccess
- AmazonDetectiveServiceLinkedRolePolicy
- AmazonDevOpsGuruConsoleFullAccess
- AmazonDevOpsGuruFullAccess
- AmazonDevOpsGuruOrganizationsAccess
- AmazonDevOpsGuruReadOnlyAccess

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

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

- AmazonEKSMCPReadOnlyAccess
- AmazonEKSNetworkingPolicy
- AmazonEKSServicePolicy
- AmazonEKSServiceRolePolicy
- AmazonEKSVPCResourceController
- AmazonEKSWorkerNodeMinimalPolicy
- AmazonEKSWorkerNodePolicy
- AmazonElastiCacheFullAccess
- AmazonElastiCacheReadOnlyAccess
- AmazonElasticContainerRegistryPublicFullAccess
- AmazonElasticContainerRegistryPublicPowerUser
- AmazonElasticContainerRegistryPublicReadOnly
- AmazonElasticFileSystemClientFullAccess
- AmazonElasticFileSystemClientReadOnlyAccess
- AmazonElasticFileSystemClientReadWriteAccess
- AmazonElasticFileSystemFullAccess
- AmazonElasticFileSystemReadOnlyAccess
- AmazonElasticFileSystemServiceRolePolicy
- AmazonElasticFileSystemsUtils
- AmazonElasticMapReduceEditorsRole
- AmazonElasticMapReduceforAutoScalingRole
- AmazonElasticMapReduceforEC2Role
- AmazonElasticMapReduceFullAccess
- AmazonElasticMapReducePlacementGroupPolicy
- AmazonElasticMapReduceReadOnlyAccess
- AmazonElasticMapReduceRole
- AmazonElasticsearchServiceRolePolicy
- AmazonElasticTranscoder_FullAccess
- AmazonElasticTranscoder_JobsSubmitter

- AmazonElasticTranscoder_ReadOnlyAccess
- AmazonElasticTranscoderRole
- AmazonEMRCleanupPolicy
- AmazonEMRContainersServiceRolePolicy
- AmazonEMRFullAccessPolicy_v2
- AmazonEMRReadOnlyAccessPolicy_v2
- AmazonEMRServerlessServiceRolePolicy
- AmazonEMRServicePolicy_v2
- AmazonESCognitoAccess
- AmazonESFullAccess
- AmazonESReadOnlyAccess
- AmazonEventBridgeApiDestinationsServiceRolePolicy
- AmazonEventBridgeFullAccess
- AmazonEventBridgePipesFullAccess
- AmazonEventBridgePipesOperatorAccess
- AmazonEventBridgePipesReadOnlyAccess
- AmazonEventBridgeReadOnlyAccess
- AmazonEventBridgeSchedulerFullAccess
- AmazonEventBridgeSchedulerReadOnlyAccess
- AmazonEventBridgeSchemasFullAccess
- AmazonEventBridgeSchemasReadOnlyAccess
- AmazonEventBridgeSchemasServiceRolePolicy
- AmazonEVSServiceRolePolicy
- AmazonFISServiceRolePolicy
- AmazonForecastFullAccess
- AmazonFraudDetectorFullAccessPolicy
- AmazonFreeRTOSFullAccess
- AmazonFreeRTOSOTAUpdate
- AmazonFSxConsoleFullAccess

- AmazonFSxConsoleReadOnlyAccess
- AmazonFSxFullAccess
- AmazonFSxReadOnlyAccess
- AmazonFSxServiceRolePolicy
- AmazonGlacierFullAccess
- AmazonGlacierReadOnlyAccess
- AmazonGrafanaAthenaAccess
- AmazonGrafanaCloudWatchAccess
- AmazonGrafanaRedshiftAccess
- AmazonGrafanaServiceLinkedRolePolicy
- AmazonGuardDutyFullAccess
- AmazonGuardDutyFullAccess_v2
- AmazonGuardDutyMalwareProtectionServiceRolePolicy
- AmazonGuardDutyReadOnlyAccess
- AmazonGuardDutyServiceRolePolicy
- AmazonHealthLakeFullAccess
- AmazonHealthLakeReadOnlyAccess
- AmazonHoneycodeFullAccess
- AmazonHoneycodeReadOnlyAccess
- AmazonHoneycodeServiceRolePolicy
- AmazonHoneycodeTeamAssociationFullAccess
- AmazonHoneycodeTeamAssociationReadOnlyAccess
- AmazonHoneycodeWorkbookFullAccess
- AmazonHoneycodeWorkbookReadOnlyAccess
- AmazonInspector2AgentlessServiceRolePolicy
- AmazonInspector2FullAccess
- AmazonInspector2FullAccess_v2
- AmazonInspector2ManagedCisPolicy
- AmazonInspector2ReadOnlyAccess

- AmazonInspector2ServiceRolePolicy
- AmazonInspectorFullAccess
- AmazonInspectorReadOnlyAccess
- AmazonInspectorServiceRolePolicy
- AmazonKendraFullAccess
- AmazonKendraReadOnlyAccess
- AmazonKeyspacesFullAccess
- AmazonKeyspacesReadOnlyAccess
- AmazonKeyspacesReadOnlyAccess_v2
- AmazonKinesisAnalyticsFullAccess
- AmazonKinesisAnalyticsReadOnly
- AmazonKinesisFirehoseFullAccess
- AmazonKinesisFirehoseReadOnlyAccess
- AmazonKinesisFullAccess
- AmazonKinesisReadOnlyAccess
- AmazonKinesisVideoStreamsFullAccess
- AmazonKinesisVideoStreamsReadOnlyAccess
- AmazonLaunchWizard_Fullaccess
- AmazonLaunchWizardFullAccessV2
- AmazonLexChannelsAccess
- AmazonLexFullAccess
- AmazonLexReadOnly
- AmazonLexReplicationPolicy
- AmazonLexRunBotsOnly
- AmazonLexV2BotPolicy
- AmazonLookoutEquipmentFullAccess
- AmazonLookoutEquipmentReadOnlyAccess
- AmazonLookoutMetricsFullAccess
- AmazonLookoutMetricsReadOnlyAccess

- AmazonLookoutVisionConsoleFullAccess
- AmazonLookoutVisionConsoleReadOnlyAccess
- AmazonLookoutVisionFullAccess
- AmazonLookoutVisionReadOnlyAccess
- AmazonMachineLearningBatchPredictionsAccess
- AmazonMachineLearningCreateOnlyAccess
- AmazonMachineLearningFullAccess
- AmazonMachineLearningManageRealTimeEndpointOnlyAccess
- AmazonMachineLearningReadOnlyAccess
- AmazonMachineLearningRealTimePredictionOnlyAccess
- AmazonMachineLearningRoleforRedshiftDataSourceV3
- AmazonMacieFullAccess
- AmazonMacieHandshakeRole
- AmazonMacieReadOnlyAccess
- AmazonMacieServiceRole
- AmazonMacieServiceRolePolicy
- AmazonManagedBlockchainConsoleFullAccess
- AmazonManagedBlockchainFullAccess
- AmazonManagedBlockchainReadOnlyAccess
- AmazonManagedBlockchainServiceRolePolicy
- AmazonMCSFullAccess
- AmazonMCSReadOnlyAccess
- AmazonMechanicalTurkFullAccess
- AmazonMechanicalTurkReadOnly
- AmazonMemoryDBFullAccess
- AmazonMemoryDBReadOnlyAccess
- AmazonMobileAnalyticsFinancialReportAccess
- AmazonMobileAnalyticsFullAccess
- AmazonMobileAnalyticsNon-financialReportAccess

- AmazonMobileAnalyticsWriteOnlyAccess
- AmazonMonitronFullAccess
- AmazonMQApiFullAccess
- AmazonMQApiReadOnlyAccess
- AmazonMQFullAccess
- AmazonMQReadOnlyAccess
- AmazonMQServiceRolePolicy
- AmazonMSKConnectReadOnlyAccess
- AmazonMSKFullAccess
- AmazonMSKReadOnlyAccess
- AmazonMWAAServerlessServiceRolePolicy
- AmazonMWAAServiceRolePolicy
- AmazonNimbleStudio-LaunchProfileWorker
- AmazonNimbleStudio-StudioAdmin
- AmazonNimbleStudio-StudioUser
- AmazonODBServiceRolePolicy
- AmazonOmicsFullAccess
- AmazonOmicsReadOnlyAccess
- AmazonOneEnterpriseFullAccess
- AmazonOneEnterpriseInstallerAccess
- AmazonOneEnterpriseReadOnlyAccess
- AmazonOpenSearchDashboardsServiceRolePolicy
- AmazonOpenSearchDirectQueryGlueCreateAccess
- AmazonOpenSearchIngestionFullAccess
- AmazonOpenSearchIngestionReadOnlyAccess
- AmazonOpenSearchIngestionServiceRolePolicy
- AmazonOpenSearchServerlessServiceRolePolicy
- AmazonOpenSearchServiceCognitoAccess
- AmazonOpenSearchServiceFullAccess

- AmazonOpenSearchServiceReadOnlyAccess
- AmazonOpenSearchServiceRolePolicy
- AmazonPersonalizeFullAccess
- AmazonPollyFullAccess
- AmazonPollyReadOnlyAccess
- AmazonPrometheusConsoleFullAccess
- AmazonPrometheusFullAccess
- AmazonPrometheusQueryAccess
- AmazonPrometheusRemoteWriteAccess
- AmazonPrometheusScraperServiceRolePolicy
- AmazonQDeveloperAccess
- AmazonQFullAccess
- AmazonQLDBConsoleFullAccess
- AmazonQLDBFullAccess
- AmazonQLDBReadOnly
- AmazonRDSBetaServiceRolePolicy
- AmazonRDSCustomInstanceProfileRolePolicy
- AmazonRDSCustomPreviewServiceRolePolicy
- AmazonRDSCustomServiceRolePolicy
- AmazonRDSDataFullAccess
- AmazonRDSDirectoryServiceAccess
- AmazonRDSEnhancedMonitoringRole
- AmazonRDSFullAccess
- AmazonRDSPerformanceInsightsFullAccess
- AmazonRDSPerformanceInsightsReadOnly
- AmazonRDSPreviewServiceRolePolicy
- AmazonRDSReadOnlyAccess
- AmazonRDSServiceRolePolicy
- AmazonRedshiftAllCommandsFullAccess

- AmazonRedshiftDataFullAccess
- AmazonRedshiftFederatedAuthorization
- AmazonRedshiftFullAccess
- AmazonRedshiftQueryEditor
- AmazonRedshiftQueryEditorV2FullAccess
- AmazonRedshiftQueryEditorV2NoSharing
- AmazonRedshiftQueryEditorV2ReadSharing
- AmazonRedshiftQueryEditorV2ReadWriteSharing
- AmazonRedshiftReadOnlyAccess
- AmazonRedshiftServiceLinkedRolePolicy
- AmazonRekognitionCustomLabelsFullAccess
- AmazonRekognitionFullAccess
- AmazonRekognitionReadOnlyAccess
- AmazonRekognitionServiceRole
- AmazonRoute53AutoNamingFullAccess
- AmazonRoute53AutoNamingReadOnlyAccess
- AmazonRoute53AutoNamingRegistrantAccess
- AmazonRoute53DomainsFullAccess
- AmazonRoute53DomainsReadOnlyAccess
- AmazonRoute53FullAccess
- AmazonRoute53ProfilesFullAccess
- AmazonRoute53ProfilesReadOnlyAccess
- AmazonRoute53ReadOnlyAccess
- AmazonRoute53RecoveryClusterFullAccess
- AmazonRoute53RecoveryClusterReadOnlyAccess
- AmazonRoute53RecoveryControlConfigFullAccess
- AmazonRoute53RecoveryControlConfigReadOnlyAccess
- AmazonRoute53RecoveryReadinessFullAccess
- AmazonRoute53RecoveryReadinessReadOnlyAccess

- AmazonRoute53ResolverFullAccess
- AmazonRoute53ResolverReadOnlyAccess
- AmazonS3FullAccess
- AmazonS3ObjectLambdaExecutionRolePolicy
- AmazonS3OutpostsFullAccess
- AmazonS3OutpostsReadOnlyAccess
- AmazonS3ReadOnlyAccess
- AmazonS3TablesFullAccess
- AmazonS3TablesLakeFormationServiceRole
- AmazonS3TablesReadOnlyAccess
- AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy
- AmazonSageMakerCanvasAIServicesAccess
- AmazonSageMakerCanvasBedrockAccess
- AmazonSageMakerCanvasDataPrepFullAccess
- AmazonSageMakerCanvasDirectDeployAccess
- AmazonSageMakerCanvasEMRServerlessExecutionRolePolicy
- AmazonSageMakerCanvasForecastAccess
- AmazonSageMakerCanvasFullAccess
- AmazonSageMakerCanvasSMDataScienceAssistantAccess
- AmazonSageMakerClusterInstanceRolePolicy
- AmazonSageMakerCoreServiceRolePolicy
- AmazonSageMakerEdgeDeviceFleetPolicy
- AmazonSageMakerFeatureStoreAccess
- AmazonSageMakerFullAccess
- AmazonSageMakerGeospatialExecutionRole
- AmazonSageMakerGeospatialFullAccess
- AmazonSageMakerGroundTruthExecution
- AmazonSageMakerHyperPodObservabilityAdminAccess
- AmazonSageMakerHyperPodServiceRolePolicy

- AmazonSageMakerHyperPodTrainingOperatorAccess
- AmazonSageMakerMechanicalTurkAccess
- AmazonSageMakerModelGovernanceUseAccess
- AmazonSageMakerModelRegistryFullAccess
- AmazonSageMakerNotebooksServiceRolePolicy
- AmazonSageMakerPartnerAppsFullAccess
- AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy
- AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy
- AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy
- AmazonSageMakerPipelinesIntegrations
- AmazonSageMakerQuickSightVPCPolicy
- AmazonSageMakerReadOnly
- AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy
- AmazonSageMakerSpacesControllerPolicy
- AmazonSageMakerSpacesRouterPolicy
- AmazonSageMakerTrainingPlanCreateAccess
- AmazonSecurityLakeAdministrator
- AmazonSecurityLakeMetastoreManager
- AmazonSecurityLakePermissionsBoundary
- AmazonSESFullAccess
- AmazonSESReadOnlyAccess
- AmazonSESServiceRolePolicy

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

- AmazonVPCFullAccess
- AmazonVPCNetworkAccessAnalyzerFullAccessPolicy
- AmazonVPCReachabilityAnalyzerFullAccessPolicy
- AmazonVPCReachabilityAnalyzerPathComponentReadPolicy
- AmazonVPCReadOnlyAccess
- AmazonWorkDocsFullAccess
- AmazonWorkDocsReadOnlyAccess
- AmazonWorkMailEventsServiceRolePolicy
- AmazonWorkMailFullAccess
- AmazonWorkMailMessageFlowFullAccess
- AmazonWorkMailMessageFlowReadOnlyAccess
- AmazonWorkMailReadOnlyAccess
- AmazonWorkSpacesAdmin
- AmazonWorkSpacesApplicationManagerAdminAccess
- AmazonWorkspacesPCAAccess
- AmazonWorkSpacesPoolServiceAccess
- AmazonWorkSpacesSecureBrowserReadOnly
- AmazonWorkSpacesSelfServiceAccess
- AmazonWorkSpacesServiceAccess
- AmazonWorkSpacesThinClientFullAccess
- AmazonWorkSpacesThinClientMonitoringServiceRolePolicy
- AmazonWorkSpacesThinClientReadOnlyAccess
- AmazonWorkSpacesWebReadOnly
- AmazonWorkSpacesWebServiceRolePolicy
- AmazonZocaloFullAccess
- AmazonZocaloReadOnlyAccess
- AmplifyBackendDeployFullAccess
- APIGatewayServiceRolePolicy
- AppIntegrationsServiceLinkedRolePolicy

- ApplicationAutoScalingForAmazonAppStreamAccess
- ApplicationDiscoveryServiceContinuousExportServiceRolePolicy
- AppRunnerNetworkingServiceRolePolicy
- AppRunnerServiceRolePolicy
- AppStudioServiceRolePolicy
- AuroraDsqlServiceLinkedRolePolicy
- AutoScalingConsoleFullAccess
- AutoScalingConsoleReadOnlyAccess
- AutoScalingFullAccess
- AutoScalingNotificationAccessRole
- AutoScalingReadOnlyAccess
- AutoScalingServiceRolePolicy
- AWS-SSM-Automation-DiagnosisBucketPolicy
- AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy
- AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy
- AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrationRolePolicy
- AWS-SSM-RemediationAutomation-AdministrationRolePolicy
- AWS-SSM-RemediationAutomation-ExecutionRolePolicy
- AWS-SSM-RemediationAutomation-OperationalAccountAdministrationRolePolicy
- AWS_ConfigRole
- AWSAccountActivityAccess
- AWSAccountManagementFullAccess
- AWSAccountManagementReadOnlyAccess
- AWSAccountSettingsManagementRole
- AWSAccountUsageReportAccess
- AWSAgentlessDiscoveryService
- AWSAppFabricFullAccess
- AWSAppFabricReadOnlyAccess
- AWSAppFabricServiceRolePolicy

- AWSApplicationAutoscalingAppStreamFleetPolicy
- AWSApplicationAutoscalingCassandraTablePolicy
- AWSApplicationAutoscalingComprehendEndpointPolicy
- AWSApplicationAutoScalingCustomResourcePolicy
- AWSApplicationAutoscalingDynamoDBTablePolicy
- AWSApplicationAutoscalingEC2SpotFleetRequestPolicy
- AWSApplicationAutoscalingECSServicePolicy
- AWSApplicationAutoscalingElastiCacheRGPolicy
- AWSApplicationAutoscalingEMRInstanceGroupPolicy
- AWSApplicationAutoscalingKafkaClusterPolicy
- AWSApplicationAutoscalingLambdaConcurrencyPolicy
- AWSApplicationAutoscalingNeptuneClusterPolicy
- AWSApplicationAutoscalingRDSClusterPolicy
- AWSApplicationAutoscalingSageMakerEndpointPolicy
- AWSApplicationAutoscalingWorkSpacesPoolPolicy
- AWSApplicationDiscoveryAgentAccess
- AWSApplicationDiscoveryAgentlessCollectorAccess
- AWSApplicationDiscoveryServiceFullAccess
- AWSApplicationMigrationAgentInstallationPolicy
- AWSApplicationMigrationAgentPolicy
- AWSApplicationMigrationAgentPolicy_v2
- AWSApplicationMigrationConversionServerPolicy
- AWSApplicationMigrationEC2Access
- AWSApplicationMigrationFullAccess
- AWSApplicationMigrationMGHAccess
- AWSApplicationMigrationNetworkMigrationCustomResource
- AWSApplicationMigrationNetworkMigrationMultiAccount
- AWSApplicationMigrationReadOnlyAccess
- AWSApplicationMigrationReplicationServerPolicy

- AWSApplicationMigrationServiceEc2InstancePolicy
- AWSApplicationMigrationServiceRolePolicy
- AWSApplicationMigrationSSMAccess
- AWSApplicationMigrationVCenterClientPolicy
- AWSAppMeshEnvoyAccess
- AWSAppMeshFullAccess
- AWSAppMeshPreviewEnvoyAccess
- AWSAppMeshPreviewServiceRolePolicy
- AWSAppMeshReadOnly
- AWSAppMeshServiceRolePolicy
- AWSAppRunnerFullAccess
- AWSAppRunnerReadOnlyAccess
- AWSAppRunnerServicePolicyForECRAccess
- AWSAppSyncAdministrator
- AWSAppSyncInvokeFullAccess
- AWSAppSyncPushToCloudWatchLogs
- AWSAppSyncSchemaAuthor
- AWSAppSyncServiceRolePolicy
- AWSArtifactAccountSync
- AWSArtifactAgreementsFullAccess
- AWSArtifactAgreementsReadOnlyAccess
- AWSArtifactReportsReadOnlyAccess
- AWSArtifactServiceRolePolicy
- AWSAuditManagerAdministratorAccess
- AWSAuditManagerServiceRolePolicy
- AWSAutoScalingPlansEC2AutoScalingPolicy
- AWSBackupAuditAccess
- AWSBackupDataTransferAccess
- AWSBackupFullAccess

- AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync
- AWSBackupGuardDutyRolePolicyForScans
- AWSBackupOperatorAccess
- AWSBackupOrganizationAdminAccess
- AWSBackupRestoreAccessForSAPHANA
- AWSBackupSearchOperatorAccess
- AWSBackupServiceLinkedRolePolicyForBackup
- AWSBackupServiceLinkedRolePolicyForBackupTest
- AWSBackupServiceRolePolicyForBackup
- AWSBackupServiceRolePolicyForIndexing
- AWSBackupServiceRolePolicyForItemRestores
- AWSBackupServiceRolePolicyForRestores
- AWSBackupServiceRolePolicyForS3Backup
- AWSBackupServiceRolePolicyForS3Restore
- AWSBackupServiceRolePolicyForScans
- AWSBatchFullAccess
- AWSBatchServiceEventTargetRole
- AWSBatchServiceRole
- AWSBatchServiceRolePolicyForSageMaker
- AWSBCMDataExportsServiceRolePolicy
- AWSBillingConductorFullAccess
- AWSBillingConductorReadOnlyAccess
- AWSBillingReadOnlyAccess
- AWSBillingServiceRolePolicy
- AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM
- AWSBudgetsActionsWithAWSResourceControlAccess
- AWSBudgetsReadOnlyAccess
- AWSBugBustFullAccess
- AWSBugBustPlayerAccess

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

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

- AWSCodeStarServiceRole
- AWSCompromisedKeyQuarantine
- AWSCompromisedKeyQuarantineV2
- AWSCompromisedKeyQuarantineV3
- AWSConfigMultiAccountSetupPolicy
- AWSConfigRemediationServiceRolePolicy
- AWSConfigRoleForOrganizations
- AWSConfigRulesExecutionRole
- AWSConfigServiceRolePolicy
- AWSConfigUserAccess
- AWSConnector
- AWSControlTowerAccountServiceRolePolicy
- AWSControlTowerCloudTrailRolePolicy
- AWSControlTowerIdentityCenterManagementPolicy
- AWSControlTowerServiceRolePolicy
- AWSCostAndUsageReportAutomationPolicy
- AWSDataExchangeDataGrantOwnerFullAccess
- AWSDataExchangeDataGrantReceiverFullAccess
- AWSDataExchangeFullAccess
- AWSDataExchangeProviderFullAccess
- AWSDataExchangeReadOnly
- AWSDataExchangeServiceRolePolicyForLicenseManagement
- AWSDataExchangeServiceRolePolicyForOrganizationDiscovery
- AWSDataExchangeSubscriberFullAccess
- AWSDataLifecycleManagerServiceRole
- AWSDataLifecycleManagerServiceRoleForAMIManagement
- AWSDataLifecycleManagerSSMFullAccess
- AWSDataPipeline_FullAccess
- AWSDataPipeline_PowerUser
- AWSDataSyncDiscoveryServiceRolePolicy

- AWSDataSyncFullAccess
- AWSDataSyncReadOnlyAccess
- AWSDataSyncServiceRolePolicy
- AWSDeadlineCloud-FleetWorker
- AWSDeadlineCloud-UserAccessFarms
- AWSDeadlineCloud-UserAccessFleets
- AWSDeadlineCloud-UserAccessJobs
- AWSDeadlineCloud-UserAccessQueues
- AWSDeadlineCloud-WorkerHost
- AWSDeepLensLambdaFunctionAccessPolicy
- AWSDeepLensServiceRolePolicy
- AWSDeepRacerAccountAdminAccess
- AWSDeepRacerCloudFormationAccessPolicy
- AWSDeepRacerDefaultMultiUserAccess
- AWSDeepRacerFullAccess
- AWSDeepRacerRoboMakerAccessPolicy
- AWSDeepRacerServiceRolePolicy
- AWSDenyAll
- AWSDeviceFarmFullAccess
- AWSDeviceFarmServiceRolePolicy
- AWSDeviceFarmTestGridServiceRolePolicy
- AWSDirectConnectFullAccess
- AWSDirectConnectReadOnlyAccess
- AWSDirectConnectServiceRolePolicy
- AWSDirectoryServiceDataFullAccess
- AWSDirectoryServiceDataReadOnlyAccess
- AWSDirectoryServiceFullAccess
- AWSDirectoryServiceReadOnlyAccess
- AWSDirectoryServiceServiceRolePolicy
- AWSDiscoveryContinuousExportFirehosePolicy

- AWSDMSFleetAdvisorServiceRolePolicy
- AWSDMSServerlessServiceRolePolicy
- AWSEC2CapacityManagerServiceRolePolicy
- AWSEC2CapacityReservationFleetRolePolicy
- AWSEC2FleetServiceRolePolicy
- AWSEC2SpotFleetServiceRolePolicy
- AWSEC2SpotServiceRolePolicy
- AWSEC2SqlHaInstancePolicy
- AWSEC2SqlHaServiceRolePolicy
- AWSEC2VssSnapshotPolicy
- AWSECRPullThroughCache_ServiceRolePolicy
- AWSElasticBeanstalkCustomPlatformforEC2Role
- AWSElasticBeanstalkEnhancedHealth
- AWSElasticBeanstalkMaintenance
- AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy
- AWSElasticBeanstalkManagedUpdatesServiceRolePolicy
- AWSElasticBeanstalkMulticontainerDocker
- AWSElasticBeanstalkReadOnly
- AWSElasticBeanstalkRoleCore
- AWSElasticBeanstalkRoleCWL
- AWSElasticBeanstalkRoleECS
- AWSElasticBeanstalkRoleRDS
- AWSElasticBeanstalkRoleSNS
- AWSElasticBeanstalkRoleWorkerTier
- AWSElasticBeanstalkService
- AWSElasticBeanstalkServiceRolePolicy
- AWSElasticBeanstalkWebTier
- AWSElasticBeanstalkWorkerTier
- AWSElasticDisasterRecoveryAgentInstallationPolicy
- AWSElasticDisasterRecoveryAgentPolicy

- AWSElasticDisasterRecoveryConsoleFullAccess
- AWSElasticDisasterRecoveryConsoleFullAccess_v2
- AWSElasticDisasterRecoveryConversionServerPolicy
- AWSElasticDisasterRecoveryCrossAccountReplicationPolicy
- AWSElasticDisasterRecoveryEc2InstancePolicy
- AWSElasticDisasterRecoveryFailbackInstallationPolicy
- AWSElasticDisasterRecoveryFailbackPolicy
- AWSElasticDisasterRecoveryLaunchActionsPolicy
- AWSElasticDisasterRecoveryNetworkReplicationPolicy
- AWSElasticDisasterRecoveryReadOnlyAccess
- AWSElasticDisasterRecoveryRecoveryInstancePolicy
- AWSElasticDisasterRecoveryReplicationServerPolicy
- AWSElasticDisasterRecoveryServiceRolePolicy
- AWSElasticDisasterRecoveryStagingAccountPolicy
- AWSElasticDisasterRecoveryStagingAccountPolicy_v2
- AWSElasticLoadBalancingClassicServiceRolePolicy
- AWSElasticLoadBalancingServiceRolePolicy
- AWSElementalMediaConnectFullAccess
- AWSElementalMediaConnectReadOnlyAccess
- AWSElementalMediaConvertFullAccess
- AWSElementalMediaConvertReadOnly
- AWSElementalMediaLiveFullAccess
- AWSElementalMediaLiveReadOnly
- AWSElementalMediaPackageFullAccess
- AWSElementalMediaPackageReadOnly
- AWSElementalMediaPackageV2FullAccess
- AWSElementalMediaPackageV2ReadOnly
- AWSElementalMediaStoreFullAccess
- AWSElementalMediaStoreReadOnly
- AWSElementalMediaTailorFullAccess

- AWSElementalMediaTailorReadOnly
- AWSEnhancedClassicNetworkingMangementPolicy
- AWSEntityResolutionConsoleFullAccess
- AWSEntityResolutionConsoleReadOnlyAccess
- AWSFaultInjectionSimulatorEC2Access
- AWSFaultInjectionSimulatorECSAccess
- AWSFaultInjectionSimulatorEKSAccess
- AWSFaultInjectionSimulatorNetworkAccess
- AWSFaultInjectionSimulatorRDSAccess
- AWSFaultInjectionSimulatorSSMAccess
- AWSFinSpaceServiceRolePolicy
- AWSFMAdminFullAccess
- AWSFMAdminReadOnlyAccess
- AWSFMMemberReadOnlyAccess
- AWSForWordPressPluginPolicy
- AWSGitSyncServiceRolePolicy
- AWSGlobalAcceleratorSLRPolicy
- AWSGlueConsoleFullAccess
- AWSGlueConsoleSageMakerNotebookFullAccess
- AwsGlueDataBrewFullAccessPolicy
- AWSGlueDataBrewServiceRole
- AWSGlueSchemaRegistryFullAccess
- AWSGlueSchemaRegistryReadonlyAccess
- AWSGlueServiceNotebookRole
- AWSGlueServiceRole
- AwsGlueSessionUserRestrictedNotebookPolicy
- AwsGlueSessionUserRestrictedNotebookServiceRole
- AwsGlueSessionUserRestrictedPolicy
- AwsGlueSessionUserRestrictedServiceRole
- AWSGrafanaAccountAdministrator

- AWSGrafanaConsoleReadOnlyAccess
- AWSGrafanaWorkspacePermissionManagement
- AWSGrafanaWorkspacePermissionManagementV2
- AWSGreengrassFullAccess
- AWSGreengrassReadOnlyAccess
- AWSGreengrassResourceAccessRolePolicy
- AWSGroundStationAgentInstancePolicy
- AWSHealth_EventProcessorServiceRolePolicy
- AWSHealthFullAccess
- AWSHealthImagingFullAccess
- AWSHealthImagingReadOnlyAccess
- AWSIAMIdentityCenterAllowListForIdentityContext
- AWSIdentityCenterExternalManagementPolicy
- AWSIdentitySyncFullAccess
- AWSIdentitySyncReadOnlyAccess
- AWSImageBuilderFullAccess
- AWSImageBuilderReadOnlyAccess
- AWSImportExportFullAccess
- AWSImportExportReadOnlyAccess
- AWSIncidentManagerIncidentAccessServiceRolePolicy
- AWSIncidentManagerResolverAccess
- AWSIncidentManagerServiceRolePolicy
- AWSIoT1ClickFullAccess
- AWSIoT1ClickReadOnlyAccess
- AWSIoTAnalyticsFullAccess
- AWSIoTAnalyticsReadOnlyAccess
- AWSIoTConfigAccess
- AWSIoTConfigReadOnlyAccess
- AWSIoTDataAccess
- AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction

- AWSIoTDeviceDefenderAudit
- AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction
- AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction
- AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction
- AWSIoTDeviceDefenderUpdateCACertMitigationAction
- AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction
- AWSIoTDeviceTesterForFreeRTOSFullAccess
- AWSIoTDeviceTesterForGreengrassFullAccess
- AWSIoTEventsFullAccess
- AWSIoTEventsReadOnlyAccess
- AWSIoTFleetHubFederationAccess
- AWSIoTFleetwiseServiceRolePolicy
- AWSIoTFullAccess
- AWSIoTLogging
- AWSIoTManagedIntegrationsFullAccess
- AWSIoTManagedIntegrationsRolePolicy
- AWSIoTOTAUpdate
- AWSIotRoboRunnerFullAccess
- AWSIotRoboRunnerReadOnly
- AWSIotRoboRunnerServiceRolePolicy
- AWSIoTRuleActions
- AWSIoTSiteWiseConsoleFullAccess
- AWSIoTSiteWiseFullAccess
- AWSIoTSiteWiseMonitorPortalAccess
- AWSIoTSiteWiseMonitorServiceRolePolicy
- AWSIoTSiteWiseReadOnlyAccess
- AWSIoTThingsRegistration
- AWSIoTTwinMakerServiceRolePolicy
- AWSIoTWirelessDataAccess
- AWSIoTWirelessFullAccess

- AWSIoTWirelessFullPublishAccess
- AWSIoTWirelessGatewayCertManager
- AWSIoTWirelessLogging
- AWSIoTWirelessReadOnlyAccess
- AWSIPAMServiceRolePolicy
- AWSIQContractServiceRolePolicy
- AWSIQFullAccess
- AWSIQPermissionServiceRolePolicy
- AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy
- AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy
- AWSKeyManagementServicePowerUser
- AWSLakeFormationCrossAccountManager
- AWSLakeFormationDataAdmin
- AWSLambda_FullAccess
- AWSLambda_ReadOnlyAccess
- AWSLambdaBasicDurableExecutionRolePolicy
- AWSLambdaBasicExecutionRole
- AWSLambdaDynamoDBExecutionRole
- AWSLambdaENIManagementAccess
- AWSLambdaExecute
- AWSLambdaFullAccess
- AWSLambdaInvocation-DynamoDB
- AWSLambdaKinesisExecutionRole
- AWSLambdaManagedEC2ResourceOperator
- AWSLambdaMSKExecutionRole
- AWSLambdaReplicator
- AWSLambdaRole
- AWSLambdaServiceRolePolicy
- AWSLambdaSQSQueueExecutionRole
- AWSLambdaVPCAccessExecutionRole

- AWSLicenseManagerConsumptionPolicy
- AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy
- AWSLicenseManagerMasterAccountRolePolicy
- AWSLicenseManagerMemberAccountRolePolicy
- AWSLicenseManagerServiceRolePolicy
- AWSLicenseManagerUserSubscriptionsServiceRolePolicy
- AWSM2ServicePolicy
- AWSManagedServices_ContactsServiceRolePolicy
- AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy
- AWSManagedServices_EventsServiceRolePolicy
- AWSManagedServices_SelfServiceReporting_ServiceRolePolicy
- AWSManagedServicesDeploymentToolkitPolicy
- AWSManagementConsoleAdministratorAccess
- AWSManagementConsoleBasicUserAccess
- AWSMarketplaceAmiIngestion
- AWSMarketplaceDeploymentServiceRolePolicy
- AWSMarketplaceFullAccess
- AWSMarketplaceGetEntitlements
- AWSMarketplaceImageBuildFullAccess
- AWSMarketplaceLicenseManagementServiceRolePolicy
- AWSMarketplaceManageSubscriptions
- AWSMarketplaceMeteringFullAccess
- AWSMarketplaceMeteringRegisterUsage
- AWSMarketplaceProcurementSystemAdminFullAccess
- AWSMarketplacePurchaseOrdersServiceRolePolicy
- AWSMarketplaceRead-only
- AWSMarketplaceResaleAuthorizationServiceRolePolicy
- AWSMarketplaceSellerFullAccess
- AWSMarketplaceSellerOfferManagement
- AWSMarketplaceSellerProductsFullAccess

- AWSMarketplaceSellerProductsReadOnly
- AWSMcpServiceActionsFullAccess
- AWSMediaConnectServicePolicy
- AWSMediaLiveAnywhereServiceRolePolicy
- AWSMediaTailorServiceRolePolicy
- AWSMigrationHubDiscoveryAccess
- AWSMigrationHubDMSAccess
- AWSMigrationHubFullAccess
- AWSMigrationHubOrchestratorConsoleFullAccess
- AWSMigrationHubOrchestratorInstanceRolePolicy
- AWSMigrationHubOrchestratorPlugin
- AWSMigrationHubOrchestratorServiceRolePolicy
- AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess
- AWSMigrationHubRefactorSpaces-SSMAutomationPolicy
- AWSMigrationHubRefactorSpacesFullAccess
- AWSMigrationHubRefactorSpacesServiceRolePolicy
- AWSMigrationHubSMSAccess
- AWSMigrationHubStrategyCollector
- AWSMigrationHubStrategyConsoleFullAccess
- AWSMigrationHubStrategyServiceRolePolicy
- AWSMobileHub_FullAccess
- AWSMobileHub_ReadOnly
- AWSMSKReplicatorExecutionRole
- AWSNATGatewayServiceRolePolicy
- AWSNetworkFirewallFullAccess
- AWSNetworkFirewallReadOnlyAccess
- AWSNetworkFirewallServiceRolePolicy
- AWSNetworkManagerCloudWANServiceRolePolicy
- AWSNetworkManagerFullAccess
- AWSNetworkManagerReadOnlyAccess

- AWSNetworkManagerServiceRolePolicy
- AWSObservabilityAdminLogsCentralizationServiceRolePolicy
- AWSObservabilityAdminServiceRolePolicy
- AWSObservabilityAdminTelemetryEnablementServiceRolePolicy
- AWSOrganizationsFullAccess
- AWSOrganizationsReadOnlyAccess
- AWSOrganizationsServiceTrustPolicy
- AWSOutpostsAuthorizeServerPolicy
- AWSOutpostsServiceRolePolicy
- AWSPanoramaApplianceRolePolicy
- AWSPanoramaApplianceServiceRolePolicy
- AWSPanoramaFullAccess
- AWSPanoramaGreengrassGroupRolePolicy
- AWSPanoramaSageMakerRolePolicy
- AWSPanoramaServiceLinkedRolePolicy
- AWSPanoramaServiceRolePolicy
- AWSPartnerCentralChannelHandshakeApprovalManagement
- AWSPartnerCentralChannelManagement
- AWSPartnerCentralFullAccess
- AWSPartnerCentralMarketingManagement
- AWSPartnerCentralOpportunityManagement
- AWSPartnerCentralSandboxFullAccess
- AWSPartnerCentralSellingResourceSnapshotJobExecutionRolePolicy
- AWSPartnerLedSupportReadOnlyAccess
- AWSPCSComputeNodePolicy
- AWSPCSServiceRolePolicy
- AWSPriceListServiceFullAccess
- AWSPrivateCAAuditor
- AWSPrivateCAConnectorForKubernetesPolicy
- AWSPrivateCAFullAccess

- AWSPrivateCAPrivilegedUser
- AWSPrivateCAReadOnly
- AWSPrivateCAUser
- AWSPrivateMarketplaceAdminFullAccess
- AWSPrivateMarketplaceRequests
- AWSPrivateNetworksServiceRolePolicy
- AWSProtonCodeBuildProvisioningBasicAccess
- AWSProtonCodeBuildProvisioningServiceRolePolicy
- AWSProtonDeveloperAccess
- AWSProtonFullAccess
- AWSProtonReadOnlyAccess
- AWSProtonServiceGitSyncServiceRolePolicy
- AWSProtonSyncServiceRolePolicy
- AWSPurchaseOrdersServiceRolePolicy
- AWSQuickSetupCFGCPacksPermissionsBoundary
- AWSQuickSetupDeploymentRolePolicy
- AWSQuickSetupDevOpsGuruPermissionsBoundary
- AWSQuickSetupDistributorPermissionsBoundary
- AWSQuickSetupEnableAREXExecutionPolicy
- AWSQuickSetupEnableDHMCExecutionPolicy
- AWSQuickSetupJITNADeploymentRolePolicy
- AWSQuickSetupManagedInstanceProfileExecutionPolicy
- AWSQuickSetupManageJITNAResourcesExecutionPolicy
- AWSQuickSetupPatchPolicyBaselineAccess
- AWSQuickSetupPatchPolicyDeploymentRolePolicy
- AWSQuickSetupPatchPolicyPermissionsBoundary
- AWSQuickSetupSchedulerPermissionsBoundary
- AWSQuickSetupSSMDeploymentRolePolicy
- AWSQuickSetupSSMDeploymentS3BucketRolePolicy
- AWSQuickSetupSSMHostMgmtPermissionsBoundary

- AWSQuickSetupSSMLifecycleManagementExecutionPolicy
- AWSQuickSetupSSMManageResourcesExecutionPolicy
- AWSQuickSetupStartSSMAssociationsExecutionPolicy
- AWSQuickSetupStartStopInstancesExecutionPolicy
- AWSQuickSightAssetBundleExportPolicy
- AWSQuickSightAssetBundleImportPolicy
- AWSQuicksightAthenaAccess
- AWSQuickSightDescribeRDS
- AWSQuickSightDescribeRedshift
- AWSQuickSightElasticsearchPolicy
- AWSQuickSightIoTAnalyticsAccess
- AWSQuickSightListIAM
- AWSQuicksightOpenSearchPolicy
- AWSQuickSightSageMakerPolicy
- AWSQuickSightSecretsManagerWriteAccess
- AWSQuickSightSecretsManagerWritePolicy
- AWSQuickSightTimestreamPolicy
- AWSReachabilityAnalyzerServiceRolePolicy
- AWSRefactoringToolkitFullAccess
- AWSRefactoringToolkitSidecarPolicy
- AWSrePostPrivateCloudWatchAccess
- AWSRepostSpaceSupportOperationsPolicy
- AWSResilienceHubAsssessmentExecutionPolicy
- AWSResourceAccessManagerFullAccess
- AWSResourceAccessManagerReadOnlyAccess
- AWSResourceAccessManagerResourceShareParticipantAccess
- AWSResourceAccessManagerServiceRolePolicy
- AWSResourceExplorerFullAccess
- AWSResourceExplorerOrganizationsAccess
- AWSResourceExplorerReadOnlyAccess

- AWSResourceExplorerServiceRolePolicy
- AWSResourceGroupsReadOnlyAccess
- AWSRoboMaker_FullAccess
- AWSRoboMakerReadOnlyAccess
- AWSRoboMakerServicePolicy
- AWSRoboMakerServiceRolePolicy
- AWSRolesAnywhereFullAccess
- AWSRolesAnywhereReadOnly
- AWSRolesAnywhereServicePolicy
- AWSS3OnOutpostsServiceRolePolicy
- AWSSavingsPlansFullAccess
- AWSSavingsPlansReadOnlyAccess
- AWSSecretsManagerClientReadOnlyAccess
- AWSSecurityHubFullAccess
- AWSSecurityHubOrganizationsAccess
- AWSSecurityHubReadOnlyAccess
- AWSSecurityHubServiceRolePolicy
- AWSSecurityHubV2ServiceRolePolicy
- AWSSecurityIncidentResponseCaseFullAccess
- AWSSecurityIncidentResponseFullAccess
- AWSSecurityIncidentResponseReadOnlyAccess
- AWSSecurityIncidentResponseServiceRolePolicy
- AWSSecurityIncidentResponseTriageServiceRolePolicy
- AWSServiceCatalogAdminFullAccess
- AWSServiceCatalogAdminReadOnlyAccess
- AWSServiceCatalogAppRegistryFullAccess
- AWSServiceCatalogAppRegistryReadOnlyAccess
- AWSServiceCatalogAppRegistryServiceRolePolicy
- AWSServiceCatalogEndUserFullAccess
- AWSServiceCatalogEndUserReadOnlyAccess

- AWSServiceCatalogOrgsDataSyncServiceRolePolicy
- AWSServiceCatalogSyncServiceRolePolicy
- AWSServiceRoleForAmazonEKSNodegroup
- AWSServiceRoleForAmazonQDeveloper
- AWSServiceRoleForAWSTransform
- AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy
- AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy
- AWSServiceRoleForCodeGuru-Profiler
- AWSServiceRoleForCodeWhispererPolicy
- AWSServiceRoleForEC2ScheduledInstances
- AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy
- AWSServiceRoleForImageBuilder
- AWSServiceRoleForIoTSiteWise
- AWSServiceRoleForLogDeliveryPolicy
- AWSServiceRoleForMonitronPolicy
- AWSServiceRoleForNeptuneGraphPolicy
- AWSServiceRoleForPrivateMarketplaceAdminPolicy
- AWSServiceRoleForProcurementInsightsPolicy
- AWSServiceRoleForSMS
- AWSServiceRoleForUserSubscriptions
- AWSServiceRolePolicyForBackupReports
- AWSServiceRolePolicyForBackupRestoreTesting
- AWSServiceRolePolicyForWorkspacesInstances
- AWSShieldDRTAccessPolicy
- AWSShieldServiceRolePolicy
- AWSSocialMessagingServiceRolePolicy
- AWSSSMForSAPServiceLinkedRolePolicy
- AWSSSMOpsInsightsServiceRolePolicy
- AWSSSODirectoryAdministrator
- AWSSSODirectoryReadOnly

- AWSSSOMasterAccountAdministrator
- AWSSSOMemberAccountAdministrator
- AWSSSOReadOnly
- AWSSSOServiceRolePolicy
- AWSStepFunctionsConsoleFullAccess
- AWSStepFunctionsFullAccess
- AWSStepFunctionsReadOnlyAccess
- AWSStorageGatewayFullAccess
- AWSStorageGatewayReadOnlyAccess
- AWSStorageGatewayServiceRolePolicy
- AWSSupplyChainFederationAdminAccess
- AWSSupportAccess
- AWSSupportAppFullAccess
- AWSSupportAppReadOnlyAccess
- AWSSupportPlansFullAccess
- AWSSupportPlansReadOnlyAccess
- AWSSupportServiceRolePolicy
- AWSSystemsManagerAccountDiscoveryServicePolicy
- AWSSystemsManagerChangeManagementServicePolicy
- AWSSystemsManagerEnableConfigRecordingExecutionPolicy
- AWSSystemsManagerEnableExplorerExecutionPolicy
- AWSSystemsManagerForSAPFullAccess
- AWSSystemsManagerForSAPReadOnlyAccess
- AWSSystemsManagerJustInTimeAccessServicePolicy
- AWSSystemsManagerJustInTimeAccessTokenPolicy
- AWSSystemsManagerJustInTimeAccessTokenSessionPolicy
- AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy
- AWSSystemsManagerNotificationsServicePolicy
- AWSSystemsManagerOpsDataSyncServiceRolePolicy
- AWSThinkboxAssetServerPolicy

- AWSThinkboxAWSPortalAdminPolicy
- AWSThinkboxAWSPortalGatewayPolicy
- AWSThinkboxAWSPortalWorkerPolicy
- AWSThinkboxDeadlineResourceTrackerAccessPolicy
- AWSThinkboxDeadlineResourceTrackerAdminPolicy
- AWSThinkboxDeadlineSpotEventPluginAdminPolicy
- AWSThinkboxDeadlineSpotEventPluginWorkerPolicy
- AWSTransferConsoleFullAccess
- AWSTransferFullAccess
- AWSTransferLoggingAccess
- AWSTransferReadOnlyAccess
- AWSTransformApplicationDeploymentPolicy
- AWSTransformApplicationECSDeploymentPolicy
- AWSTransformCustomExecuteTransformations
- AWSTransformCustomFullAccess
- AWSTransformCustomManageTransformations
- AWSTrustedAdvisorPriorityFullAccess
- AWSTrustedAdvisorPriorityReadOnlyAccess
- AWSTrustedAdvisorReportingServiceRolePolicy
- AWSTrustedAdvisorServiceRolePolicy
- AWSUserAttributeCostAllocationPolicy
- AWSUserNotificationsServiceLinkedRolePolicy
- AWSVendorInsightsAssessorFullAccess
- AWSVendorInsightsAssessorReadOnly
- AWSVendorInsightsVendorFullAccess
- AWSVendorInsightsVendorReadOnly
- AWSVpcLatticeServiceRolePolicy
- AWSVPCS2SVpnServiceRolePolicy
- AWSVPCTransitGatewayServiceRolePolicy
- AWSVPCVerifiedAccessServiceRolePolicy

- AWSWAFConsoleFullAccess
- AWSWAFConsoleReadOnlyAccess
- AWSWAFFullAccess
- AWSWAFReadOnlyAccess
- AWSWellArchitectedDiscoveryServiceRolePolicy
- AWSWellArchitectedOrganizationsServiceRolePolicy
- AWSWickrFullAccess
- AWSXrayCrossAccountSharingConfiguration
- AWSXRayDaemonWriteAccess
- AWSXrayFullAccess
- AWSXrayReadOnlyAccess
- AWSXrayWriteOnlyAccess
- AWSZonalAutoshiftPracticeRunSLRPolicy
- AWSZoneGroupAccessManagementServiceRolePolicy
- BatchServiceRolePolicy
- BedrockAgentCoreFullAccess
- BedrockAgentCoreNetworkServiceRolePolicy
- BedrockAgentCoreRuntimeIdentityServiceRolePolicy
- Billing
- BudgetsServiceRolePolicy
- CertificateManagerServiceRolePolicy
- ClientVPNServiceConnectionsRolePolicy
- ClientVPNServiceRolePolicy
- CloudFormationStackSetsOrgAdminServiceRolePolicy
- CloudFormationStackSetsOrgMemberServiceRolePolicy
- CloudFrontFullAccess
- CloudFrontReadOnlyAccess
- CloudHSMServiceRolePolicy
- CloudSearchFullAccess
- CloudSearchReadOnlyAccess

- CloudTrailEventContext
- CloudTrailServiceRolePolicy
- CloudWatch-CrossAccountAccess
- CloudWatchActionsEC2Access
- CloudWatchAgentAdminPolicy
- CloudWatchAgentServerPolicy
- CloudWatchApplicationInsightsFullAccess
- CloudWatchApplicationInsightsReadOnlyAccess
- CloudwatchApplicationInsightsServiceLinkedRolePolicy
- CloudWatchApplicationSignalsFullAccess
- CloudWatchApplicationSignalsReadOnlyAccess
- CloudWatchApplicationSignalsServiceRolePolicy
- CloudWatchAutomaticDashboardsAccess
- CloudWatchCrossAccountSharingConfiguration
- CloudWatchEventsBuiltInTargetExecutionAccess
- CloudWatchEventsFullAccess
- CloudWatchEventsInvocationAccess
- CloudWatchEventsReadOnlyAccess
- CloudWatchEventsServiceRolePolicy
- CloudWatchFullAccess
- CloudWatchFullAccessV2
- CloudWatchInternetMonitorFullAccess
- CloudWatchInternetMonitorReadOnlyAccess
- CloudWatchInternetMonitorServiceRolePolicy
- CloudWatchLambdaApplicationSignalsExecutionRolePolicy
- CloudWatchLambdaInsightsExecutionRolePolicy
- CloudWatchLogsCrossAccountSharingConfiguration
- CloudWatchLogsFullAccess
- CloudWatchLogsReadOnlyAccess
- CloudWatchNetworkFlowMonitorAgentPublishPolicy

- CloudWatchNetworkFlowMonitorServiceRolePolicy
- CloudWatchNetworkFlowMonitorTopologyServiceRolePolicy
- CloudWatchNetworkMonitorServiceRolePolicy
- CloudWatchOpenSearchDashboardAccess
- CloudWatchOpenSearchDashboardsFullAccess
- CloudWatchReadOnlyAccess
- CloudWatchSyntheticsFullAccess
- CloudWatchSyntheticsReadOnlyAccess
- ComprehendDataAccessRolePolicy
- ComprehendFullAccess
- ComprehendMedicalFullAccess
- ComprehendReadOnly
- ComputeOptimizerAutomationServiceRolePolicy
- ComputeOptimizerReadOnlyAccess
- ComputeOptimizerServiceRolePolicy
- ConfigConformsServiceRolePolicy
- ConsoleFullAccessFromVercel
- ConsoleViewOnlyAccessFromVercel
- CostOptimizationHubAdminAccess
- CostOptimizationHubReadOnlyAccess
- CostOptimizationHubServiceRolePolicy
- CustomerProfilesServiceLinkedRolePolicy
- DatabaseAdministrator
- DataScientist
- DAXServiceRolePolicy
- DeclarativePoliciesEC2Report
- DynamoDBCloudWatchContributorInsightsServiceRolePolicy
- DynamoDBGlobalTableSettingsManagementServiceRolePolicy
- DynamoDBKinesisReplicationServiceRolePolicy
- DynamoDBReplicationServiceRolePolicy

- EC2FastLaunchFullAccess
- EC2FastLaunchServiceRolePolicy
- EC2FleetTimeShiftableServiceRolePolicy
- Ec2ImageBuilderCrossAccountDistributionAccess
- EC2ImageBuilderLifecycleExecutionPolicy
- EC2InstanceConnect
- Ec2InstanceConnectEndpoint
- EC2InstanceProfileForImageBuilder
- EC2InstanceProfileForImageBuilderECRContainerBuilds
- ECRReplicationServiceRolePolicy
- ECRTemplateServiceRolePolicy
- ElastiCacheServiceRolePolicy
- ElasticLoadBalancingFullAccess
- ElasticLoadBalancingReadOnly
- ElementalActivationsDownloadSoftwareAccess
- ElementalActivationsFullAccess
- ElementalActivationsGenerateLicenses
- ElementalActivationsReadOnlyAccess
- ElementalAppliancesSoftwareFullAccess
- ElementalAppliancesSoftwareReadOnlyAccess
- ElementalSupportCenterFullAccess
- EMRDescribeClusterPolicyForEMRWAL
- FMSServiceRolePolicy
- FSxDeleteServiceLinkedRoleAccess
- GameLiftContainerFleetPolicy
- GameLiftGameServerGroupPolicy
- GitLabDuoWithAmazonQPermissionsPolicy
- GlobalAcceleratorFullAccess
- GlobalAcceleratorReadOnlyAccess
- GreengrassOTAUpdateArtifactAccess

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

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

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

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

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

AccessAnalyzerServiceRolePolicy

説明: Access Analyzer によるリソースメタデータの分析を許可します

`AccessAnalyzerServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 12 月 2 日 17:13 UTC
- 編集日時: 2025 年 5 月 12 日 15:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AccessAnalyzerServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v17 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

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

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AccountManagementFromVercel

説明: Vercel Marketplace との統合を通じて作成されたアカウントで使用します AWS。アカウント管理、通知、コストと使用状況の分析、ID プロバイダー管理へのアクセスを提供します。

`AccountManagementFromVercel` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AccountManagementFromVercel をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 12 月 11 日 16:34 UTC
- 編集日時: 2025 年 12 月 11 日 16:34 UTC
- ARN: arn:aws:iam::aws:policy/AccountManagementFromVercel

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
      "Action" : [
        "iam:UpdateSamlProvider",
        "iam:GetSamlProvider"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/VercelInstallId" : "${aws:PrincipalTag/VercelInstallId}"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AdministratorAccess

説明: AWS サービスとリソースへのフルアクセスを提供します。

`AdministratorAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AdministratorAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:39 UTC
- 編集日時: 2015 年 2 月 6 日 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/AdministratorAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AdministratorAccess-Amplify

説明: Amplify アプリケーションに必要なリソースへの直接アクセスを明示的に許可すると同時にアカウント管理権限を付与します。

`AdministratorAccess-Amplify` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AdministratorAccess-Amplify` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 12 月 1 日 19:03 UTC
- 編集日時: 2024 年 4 月 4 日 20:35 UTC
- ARN: `arn:aws:iam::aws:policy/AdministratorAccess-Amplify`

ポリシーのバージョン

ポリシーのバージョン: v12 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AdministratorAccess-AWSElasticBeanstalk

説明: アカウント管理権限を付与します。開発者と管理者が Elastic Beanstalk AWS アプリケーションの管理に必要なリソースに直接アクセスすることを明示的に許可する

AdministratorAccess-AWSElasticBeanstalk は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AdministratorAccess-AWSElasticBeanstalk をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 1 月 22 日 19:36 UTC
- 編集日時: 2025 年 11 月 12 日 19:34 UTC
- ARN: arn:aws:iam::aws:policy/AdministratorAccess-AWSElasticBeanstalk

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:Describe*",
        "acm:List*",
        "autoscaling:Describe*",
        "cloudformation:Describe*",
        "cloudformation:Estimate*",
```

```
        "cloudformation:Get*",
        "cloudformation:List*",
        "cloudformation:Validate*",
        "cloudtrail:LookupEvents",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "codecommit:Get*",
        "codecommit:UploadArchive",
        "ec2:AllocateAddress",
        "ec2:AssociateAddress",
        "ec2:AuthorizeSecurityGroup*",
        "ec2:CreateLaunchTemplate*",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags",
        "ec2:DeleteLaunchTemplate*",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteTags",
        "ec2:Describe*",
        "ec2:DisassociateAddress",
        "ec2:ReleaseAddress",
        "ec2:RevokeSecurityGroup*",
        "ecs:CreateCluster",
        "ecs:DeRegisterTaskDefinition",
        "ecs:Describe*",
        "ecs:List*",
        "ecs:RegisterTaskDefinition",
        "elasticbeanstalk:*",
        "elasticloadbalancing:Describe*",
        "iam:GetRole",
        "iam:ListAttachedRolePolicies",
        "iam:ListInstanceProfiles",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListServerCertificates",
        "logs:Describe*",
        "rds:Describe*",
        "s3:ListAllMyBuckets",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "sqs:ListQueues"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:*"
      ],
      "Resource" : [
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/awseb-e-
*",
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/eb-*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/awseb-e-*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/eb-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CancelUpdateStack",
        "cloudformation:ContinueUpdateRollback",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:GetTemplate",
        "cloudformation:ListStackResources",
        "cloudformation:SignalResource",
        "cloudformation:TagResource",
        "cloudformation:UntagResource",
        "cloudformation:UpdateStack"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awseb-*",
        "arn:aws:cloudformation:*:*:stack/eb-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:awseb-*",
        "arn:aws:cloudwatch:*:*:alarm:eb-*"
      ]
    },
    {
```

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

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

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AddRoleToInstanceProfile",
        "iam:CreateInstanceProfile",
        "iam:CreateRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-elasticbeanstalk*",
        "arn:aws:iam::*:instance-profile/aws-elasticbeanstalk*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-elasticbeanstalk*",
      "Condition" : {
        "ArnLike" : {
          "iam:PolicyArn" : [
            "arn:aws:iam::aws:policy/AWSElasticBeanstalk*",
            "arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalk*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "elasticbeanstalk.amazonaws.com",
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn",
            "autoscaling.amazonaws.com",
            "elasticloadbalancing.amazonaws.com",
            "ecs.amazonaws.com",
            "cloudformation.amazonaws.com"
          ]
        }
```

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

```
        "rds:AuthorizeDBSecurityGroupIngress",
        "rds:CreateDBInstance",
        "rds:CreateDBSecurityGroup",
        "rds:DeleteDBInstance",
        "rds:DeleteDBSecurityGroup",
        "rds:ModifyDBInstance",
        "rds:RestoreDBInstanceFromDBSnapshot"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:db:*",
        "arn:aws:rds:*:*:secgrp:awseb-e-*",
        "arn:aws:rds:*:*:secgrp:eb-*",
        "arn:aws:rds:*:*:snapshot:*",
        "arn:aws:rds:*:*:subgrp:awseb-e-*",
        "arn:aws:rds:*:*:subgrp:eb-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:Delete*",
        "s3:Get*",
        "s3:Put*"
      ],
      "Resource" : "arn:aws:s3:::elasticbeanstalk-*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:GetBucket*",
        "s3:ListBucket",
        "s3:PutBucketPolicy",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketOwnershipControls"
      ],
      "Resource" : "arn:aws:s3:::elasticbeanstalk-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:DeleteTopic",
        "sns:GetTopicAttributes",
```

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AIOpsAssistantIncidentReportPolicy

説明: Amazon AI Operations Assistant が調査のインシデントレポートを生成するために必要なアクセス許可を提供します。

AIOpsAssistantIncidentReportPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AIOpsAssistantIncidentReportPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 10 月 10 日 22:04 UTC
- 編集日時: 2025 年 10 月 10 日 22:04 UTC
- ARN: arn:aws:iam::aws:policy/AIOpsAssistantIncidentReportPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Statement1",
      "Effect" : "Allow",
```

```
      "Action" : [
        "aiops:PutFact",
        "aiops:UpdateReport",
        "aiops:GetReport",
        "aiops:GenerateReport",
        "aiops:CreateReport",
        "aiops:GetFact",
        "aiops:ListFacts",
        "aiops:GetFactVersions",
        "aiops:GetInvestigation",
        "aiops:ListInvestigationEvents",
        "aiops:GetInvestigationEvent"
      ],
      "Resource" : [
        "arn:aws:aiops:*:*:investigation-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : [
            "${aws:ResourceAccount}"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AIOpsAssistantPolicy

説明: Amazon AI Operations Assistant が調査中に顧客 AWS リソースを分析するために必要な ReadOnly アクセス許可を提供します。

`AIOpsAssistantPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AIOpsAssistantPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 12 月 2 日 16:21 UTC
- 編集日時: 2025 年 12 月 17 日 16:49 UTC
- ARN: arn:aws:iam::aws:policy/AIOpsAssistantPolicy

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AIOPSServiceAccess",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:GetAnalyzer",
        "access-analyzer:List*",
        "acm-pca:Describe*",
        "acm-pca:GetCertificate",
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:GetCertificateAuthorityCsr",
        "acm-pca:List*",
        "acm:DescribeCertificate",
        "acm:GetAccountConfiguration",
        "airflow:List*",
        "amplify:GetApp",
        "amplify:GetBranch",
```

```
        "amplify:GetDomainAssociation",
        "amplify:List*",
        "aoss:BatchGetCollection",
        "aoss:BatchGetLifecyclePolicy",
        "aoss:BatchGetVpcEndpoint",
        "aoss:GetAccessPolicy",
        "aoss:GetSecurityConfig",
        "aoss:GetSecurityPolicy",
        "aoss:List*",
        "appconfig:GetApplication",
        "appconfig:GetConfigurationProfile",
        "appconfig:GetEnvironment",
        "appconfig:GetHostedConfigurationVersion",
        "appconfig:List*",
        "appflow:Describe*",
        "appflow:List*",
        "application-autoscaling:Describe*",
        "application-signals:BatchGetServiceLevelObjectiveBudgetReport",
        "application-signals:GetService",
        "application-signals:GetServiceLevelObjective",
        "application-signals:List*",
        "applicationinsights:Describe*",
        "applicationinsights:List*",
        "apprunner:Describe*",
        "apprunner:List*",
        "appstream:Describe*",
        "appstream:List*",
        "appsync:GetApiAssociation",
        "appsync:GetDataSource",
        "appsync:GetDomainName",
        "appsync:GetFunction",
        "appsync:GetGraphqlApi",
        "appsync:GetIntrospectionSchema",
        "appsync:GetResolver",
        "appsync:GetSourceApiAssociation",
        "appsync:List*",
        "aps:Describe*",
        "aps:List*",
        "arc-zonal-shift:GetManagedResource",
        "arc-zonal-shift:List*",
        "athena:GetCapacityAssignmentConfiguration",
        "athena:GetCapacityReservation",
        "athena:GetDataCatalog",
        "athena:GetNamedQuery",
```

```
        "athena:GetPreparedStatement",
        "athena:GetWorkGroup",
        "athena:List*",
        "auditmanager:GetAssessment",
        "auditmanager:List*",
        "autoscaling:Describe*",
        "backup-gateway:GetHypervisor",
        "backup-gateway:List*",
        "backup:Describe*",
        "backup:GetBackupPlan",
        "backup:GetBackupSelection",
        "backup:GetBackupVaultAccessPolicy",
        "backup:GetBackupVaultNotifications",
        "backup:GetRestoreTestingPlan",
        "backup:GetRestoreTestingSelection",
        "backup:List*",
        "batch:DescribeComputeEnvironments",
        "batch:DescribeJobQueues",
        "batch:DescribeSchedulingPolicies",
        "batch:List*",
        "bedrock:GetAgent",
        "bedrock:GetAgentActionGroup",
        "bedrock:GetAgentAlias",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:GetDataSource",
        "bedrock:GetGuardrail",
        "bedrock:GetKnowledgeBase",
        "bedrock:List*",
        "budgets:Describe*",
        "budgets:List*",
        "ce:Describe*",
        "ce:GetAnomalyMonitors",
        "ce:GetAnomalySubscriptions",
        "ce:List*",
        "chatbot:Describe*",
        "chatbot:GetMicrosoftTeamsChannelConfiguration",
        "chatbot:List*",
        "cleanrooms-ml:GetTrainingDataset",
        "cleanrooms-ml:List*",
        "cleanrooms:GetAnalysisTemplate",
        "cleanrooms:GetCollaboration",
        "cleanrooms:GetConfiguredTable",
        "cleanrooms:GetConfiguredTableAnalysisRule",
        "cleanrooms:GetConfiguredTableAssociation",
```

```
        "cleanrooms:GetMembership",
        "cleanrooms:List*",
        "cloudformation:Describe*",
        "cloudformation:GetResource",
        "cloudformation:GetStackPolicy",
        "cloudformation:GetTemplate",
        "cloudformation:List*",
        "cloudfront:Describe*",
        "cloudfront:GetCachePolicy",
        "cloudfront:GetCloudFrontOriginAccessIdentity",
        "cloudfront:GetContinuousDeploymentPolicy",
        "cloudfront:GetDistribution",
        "cloudfront:GetDistributionConfig",
        "cloudfront:GetFunction",
        "cloudfront:GetKeyGroup",
        "cloudfront:GetMonitoringSubscription",
        "cloudfront:GetOriginAccessControl",
        "cloudfront:GetOriginRequestPolicy",
        "cloudfront:GetPublicKey",
        "cloudfront:GetRealtimeLogConfig",
        "cloudfront:GetResponseHeadersPolicy",
        "cloudfront:List*",
        "cloudtrail:Describe*",
        "cloudtrail:GetChannel",
        "cloudtrail:GetEventDataStore",
        "cloudtrail:GetEventSelectors",
        "cloudtrail:GetInsightSelectors",
        "cloudtrail:GetQueryResults",
        "cloudtrail:GetResourcePolicy",
        "cloudtrail:GetTrail",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:List*",
        "cloudtrail:LookupEvents",
        "cloudtrail:StartQuery",
        "cloudwatch:Describe*",
        "cloudwatch:GenerateQuery",
        "cloudwatch:GetDashboard",
        "cloudwatch:GetInsightRuleReport",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:GetMetricStream",
        "cloudwatch:GetService",
        "cloudwatch:GetServiceLevelObjective",
        "cloudwatch:List*",
```

```
        "codeartifact:Describe*",
        "codeartifact:GetDomainPermissionsPolicy",
        "codeartifact:GetRepositoryPermissionsPolicy",
        "codeartifact:List*",
        "codebuild:BatchGetFleets",
        "codebuild:List*",
        "codecommit:GetRepository",
        "codecommit:GetRepositoryTriggers",
        "codedeploy:BatchGetDeployments",
        "codedeploy:BatchGetDeploymentTargets",
        "codedeploy:GetApplication",
        "codedeploy:GetDeploymentConfig",
        "codedeploy:List*",
        "codeguru-profiler:Describe*",
        "codeguru-profiler:GetNotificationConfiguration",
        "codeguru-profiler:GetPolicy",
        "codeguru-profiler:List*",
        "codeguru-reviewer:Describe*",
        "codeguru-reviewer:List*",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:List*",
        "codestar-connections:GetConnection",
        "codestar-connections:GetRepositoryLink",
        "codestar-connections:GetSyncConfiguration",
        "codestar-connections:List*",
        "codestar-notifications:Describe*",
        "codestar-notifications:List*",
        "cognito-identity:DescribeIdentityPool",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:ListIdentityPools",
        "cognito-identity:ListTagsForResource",
        "cognito-idp:AdminListGroupsForUser",
        "cognito-idp:DescribeIdentityProvider",
        "cognito-idp:DescribeResourceServer",
        "cognito-idp:DescribeRiskConfiguration",
        "cognito-idp:DescribeUserImportJob",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolDomain",
        "cognito-idp:GetGroup",
        "cognito-idp:GetLogDeliveryConfiguration",
        "cognito-idp:GetUICustomization",
        "cognito-idp:GetUserPoolMfaConfig",
        "cognito-idp:GetWebACLForResource",
```

```
        "cognito-idp:ListGroups",
        "cognito-idp:ListIdentityProviders",
        "cognito-idp:ListResourceServers",
        "cognito-idp:ListUserPoolClients",
        "cognito-idp:ListUserPools",
        "cognito-idp:ListUsers",
        "cognito-idp:ListTagsForResource",
        "comprehend:Describe*",
        "comprehend:List*",
        "config:Describe*",
        "config:GetStoredQuery",
        "config:List*",
        "connect:Describe*",
        "connect:GetTaskTemplate",
        "connect:List*",
        "databrew:Describe*",
        "databrew:List*",
        "datapipeline:Describe*",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:List*",
        "datasync:Describe*",
        "datasync:List*",
        "deadline:GetFarm",
        "deadline:GetFleet",
        "deadline:GetLicenseEndpoint",
        "deadline:GetMonitor",
        "deadline:GetQueue",
        "deadline:GetQueueEnvironment",
        "deadline:GetQueueFleetAssociation",
        "deadline:GetStorageProfile",
        "deadline:List*",
        "detective:GetMembers",
        "detective:List*",
        "devicefarm:GetDevicePool",
        "devicefarm:GetInstanceProfile",
        "devicefarm:GetNetworkProfile",
        "devicefarm:GetProject",
        "devicefarm:GetTestGridProject",
        "devicefarm:GetVPCEConfiguration",
        "devicefarm:List*",
        "devops-guru:Describe*",
        "devops-guru:GetResourceCollection",
        "devops-guru:List*",
        "dms:Describe*",
```

```
            "dms:List*",
            "ds:Describe*",
            "dynamodb:Describe*",
            "dynamodb:GetResourcePolicy",
            "dynamodb:List*",
            "ec2:Describe*",
            "ec2:GetAssociatedEnclaveCertificateIamRoles",
            "ec2:GetIpamPoolAllocations",
            "ec2:GetIpamPoolCidrs",
            "ec2:GetManagedPrefixListEntries",
            "ec2:GetNetworkInsightsAccessScopeContent",
            "ec2:GetSnapshotBlockPublicAccessState",
            "ec2:GetTransitGatewayMulticastDomainAssociations",
            "ec2:GetTransitGatewayRouteTableAssociations",
            "ec2:GetTransitGatewayRouteTablePropagations",
            "ec2:GetVerifiedAccessEndpointPolicy",
            "ec2:GetVerifiedAccessGroupPolicy",
            "ec2:GetVerifiedAccessInstanceWebAcl",
            "ec2:SearchLocalGatewayRoutes",
            "ec2:SearchTransitGatewayRoutes",
            "ecr:Describe*",
            "ecr:GetLifecyclePolicy",
            "ecr:GetRegistryPolicy",
            "ecr:GetRepositoryPolicy",
            "ecr:List*",
            "ecs:Describe*",
            "ecs:List*",
            "eks:Describe*",
            "eks:List*",
            "elasticache:Describe*",
            "elasticache:List*",
            "elasticbeanstalk:Describe*",
            "elasticbeanstalk:List*",
            "elasticfilesystem:Describe*",
            "elasticloadbalancing:GetResourcePolicy",
            "elasticloadbalancing:GetTrustStoreCaCertificatesBundle",
            "elasticloadbalancing:GetTrustStoreRevocationContent",
            "elasticloadbalancing:Describe*",
            "elasticmapreduce:Describe*",
            "elasticmapreduce:List*",
            "emr-containers:Describe*",
            "emr-containers:List*",
            "emr-serverless:GetApplication",
            "emr-serverless:List*",
```

```
        "es:Describe*",
        "es:List*",
        "events:Describe*",
        "events:List*",
        "evidently:GetExperiment",
        "evidently:GetFeature",
        "evidently:GetLaunch",
        "evidently:GetProject",
        "evidently:GetSegment",
        "evidently:List*",
        "firehose:Describe*",
        "firehose:List*",
        "fis:GetExperimentTemplate",
        "fis:GetTargetAccountConfiguration",
        "fis:List*",
        "fms:GetNotificationChannel",
        "fms:GetPolicy",
        "fms:List*",
        "forecast:Describe*",
        "forecast:List*",
        "frauddetector:BatchGetVariable",
        "frauddetector:Describe*",
        "frauddetector:GetDetectors",
        "frauddetector:GetDetectorVersion",
        "frauddetector:GetEntityTypes",
        "frauddetector:GetEventTypes",
        "frauddetector:GetExternalModels",
        "frauddetector:GetLabels",
        "frauddetector:GetListElements",
        "frauddetector:GetListsMetadata",
        "frauddetector:GetModelVersion",
        "frauddetector:GetOutcomes",
        "frauddetector:GetRules",
        "frauddetector:GetVariables",
        "frauddetector:List*",
        "fsx:Describe*",
        "gamelift:Describe*",
        "gamelift:List*",
        "globalaccelerator:Describe*",
        "globalaccelerator:List*",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetJob",
        "glue:GetRegistry",
```

```
        "glue:GetSchema",
        "glue:GetSchemaVersion",
        "glue:GetTable",
        "glue:GetTags",
        "glue:GetTrigger",
        "glue:List*",
        "glue:querySchemaVersionMetadata",
        "grafana:Describe*",
        "grafana:List*",
        "greengrass:Describe*",
        "greengrass:GetDeployment",
        "greengrass:List*",
        "groundstation:GetConfig",
        "groundstation:GetDataflowEndpointGroup",
        "groundstation:GetMissionProfile",
        "groundstation:List*",
        "guardduty:GetDetector",
        "guardduty:GetFilter",
        "guardduty:GetIPSet",
        "guardduty:GetMalwareProtectionPlan",
        "guardduty:GetMasterAccount",
        "guardduty:GetMembers",
        "guardduty:GetThreatIntelSet",
        "guardduty:List*",
        "health:DescribeEvents",
        "health:DescribeEventDetails",
        "healthlake:Describe*",
        "healthlake:List*",
        "iam:GetGroup",
        "iam:GetGroupPolicy",
        "iam:GetInstanceProfile",
        "iam:GetLoginProfile",
        "iam:GetOpenIDConnectProvider",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:GetSAMLProvider",
        "iam:GetServerCertificate",
        "iam:GetServiceLinkedRoleDeletionStatus",
        "iam:GetUser",
        "iam:GetUserPolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListOpenIDConnectProviders",
```

```
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListServerCertificates",
        "iam:ListVirtualMFADevices",
        "identitystore:DescribeGroup",
        "identitystore:DescribeGroupMembership",
        "identitystore:ListGroupMemberships",
        "identitystore:ListGroups",
        "imagebuilder:GetComponent",
        "imagebuilder:GetContainerRecipe",
        "imagebuilder:GetDistributionConfiguration",
        "imagebuilder:GetImage",
        "imagebuilder:GetImagePipeline",
        "imagebuilder:GetImageRecipe",
        "imagebuilder:GetInfrastructureConfiguration",
        "imagebuilder:GetLifecyclePolicy",
        "imagebuilder:GetWorkflow",
        "imagebuilder:List*",
        "inspector2:List*",
        "inspector:Describe*",
        "inspector:List*",
        "internetmonitor:GetMonitor",
        "internetmonitor:List*",
        "iot:Describe*",
        "iot:GetPackage",
        "iot:GetPackageVersion",
        "iot:GetPolicy",
        "iot:GetThingShadow",
        "iot:GetTopicRule",
        "iot:GetTopicRuleDestination",
        "iot:GetV2LoggingOptions",
        "iot:List*",
        "iotanalytics:Describe*",
        "iotanalytics:List*",
        "iotevents:Describe*",
        "iotevents:List*",
        "iotfleethub:Describe*",
        "iotfleethub:List*",
        "iotsitewise:Describe*",
        "iotsitewise:List*",
        "iotwireless:GetDestination",
        "iotwireless:GetDeviceProfile",
        "iotwireless:GetFuotaTask",
        "iotwireless:GetMulticastGroup",
```

```
        "iotwireless:GetNetworkAnalyzerConfiguration",
        "iotwireless:GetServiceProfile",
        "iotwireless:GetWirelessDevice",
        "iotwireless:GetWirelessGateway",
        "iotwireless:GetWirelessGatewayTaskDefinition",
        "iotwireless:List*",
        "ivs:GetChannel",
        "ivs:GetEncoderConfiguration",
        "ivs:GetPlaybackRestrictionPolicy",
        "ivs:GetRecordingConfiguration",
        "ivs:GetStage",
        "ivs:List*",
        "ivschat:GetLoggingConfiguration",
        "ivschat:GetRoom",
        "ivschat:List*",
        "kafka:Describe*",
        "kafka:GetClusterPolicy",
        "kafka:List*",
        "kafkaconnect:Describe*",
        "kafkaconnect:List*",
        "kendra:Describe*",
        "kendra:List*",
        "kinesis:Describe*",
        "kinesis:GetResourcePolicy",
        "kinesis:List*",
        "kinesisanalytics:Describe*",
        "kinesisanalytics:List*",
        "kinesisvideo:Describe*",
        "kms:DescribeKey",
        "kms:ListResourceTags",
        "kms:ListKeys",
        "kms:GetKeyRotationStatus",
        "kms:ListAliases",
        "kms:ListKeyRotations",
        "lakeformation:Describe*",
        "lakeformation:GetLFTag",
        "lakeformation:GetResourceLFTags",
        "lakeformation:List*",
        "lambda:GetAlias",
        "lambda:GetCodeSigningConfig",
        "lambda:GetEventSourceMapping",
        "lambda:GetFunction",
        "lambda:GetFunctionCodeSigningConfig",
        "lambda:GetFunctionConfiguration",
```

```
        "lambda:GetFunctionEventInvokeConfig",
        "lambda:GetFunctionRecursionConfig",
        "lambda:GetFunctionUrlConfig",
        "lambda:GetLayerVersion",
        "lambda:GetLayerVersionPolicy",
        "lambda:GetPolicy",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:GetRuntimeManagementConfig",
        "lambda:List*",
        "launchwizard:GetDeployment",
        "launchwizard:List*",
        "lex:Describe*",
        "lex:List*",
        "license-manager:GetLicense",
        "license-manager:List*",
        "lightsail:GetAlarms",
        "lightsail:GetBuckets",
        "lightsail:GetCertificates",
        "lightsail:GetContainerServices",
        "lightsail:GetDisk",
        "lightsail:GetDisks",
        "lightsail:GetInstance",
        "lightsail:GetInstances",
        "lightsail:GetLoadBalancer",
        "lightsail:GetLoadBalancers",
        "lightsail:GetLoadBalancerTlsCertificates",
        "lightsail:GetStaticIp",
        "lightsail:GetStaticIps",
        "logs:Describe*",
        "logs:FilterLogEvents",
        "logs:GetDataProtectionPolicy",
        "logs:GetDelivery",
        "logs:GetDeliveryDestination",
        "logs:GetDeliveryDestinationPolicy",
        "logs:GetDeliverySource",
        "logs:GetLogAnomalyDetector",
        "logs:GetLogDelivery",
        "logs:GetLogGroupFields",
        "logs:GetQueryResults",
        "logs:List*",
        "logs:StartQuery",
        "logs:StopLiveTail",
        "logs:StopQuery",
        "logs:TestMetricFilter",
```

```
        "lookoutmetrics:Describe*",
        "lookoutmetrics:List*",
        "lookoutvision:Describe*",
        "lookoutvision:List*",
        "m2:GetApplication",
        "m2:GetEnvironment",
        "m2:List*",
        "macie2:GetAllowList",
        "macie2:GetCustomDataIdentifier",
        "macie2:GetFindingsFilter",
        "macie2:GetMacieSession",
        "macie2:List*",
        "mediaconnect:Describe*",
        "mediaconnect:List*",
        "medialive:Describe*",
        "medialive:GetCloudWatchAlarmTemplate",
        "medialive:GetCloudWatchAlarmTemplateGroup",
        "medialive:GetEventBridgeRuleTemplate",
        "medialive:GetEventBridgeRuleTemplateGroup",
        "medialive:GetSignalMap",
        "medialive:List*",
        "mediapackage-vod:Describe*",
        "mediapackage-vod:List*",
        "mediapackage:Describe*",
        "mediapackage:List*",
        "mediapackagev2:GetChannel",
        "mediapackagev2:GetChannelGroup",
        "mediapackagev2:GetChannelPolicy",
        "mediapackagev2:GetOriginEndpoint",
        "mediapackagev2:GetOriginEndpointPolicy",
        "mediapackagev2:List*",
        "memorydb:Describe*",
        "memorydb:List*",
        "mobiletargeting:GetInAppTemplate",
        "mobiletargeting:List*",
        "mq:Describe*",
        "mq:List*",
        "network-firewall:Describe*",
        "network-firewall:List*",
        "networkmanager:Describe*",
        "networkmanager:GetConnectAttachment",
        "networkmanager:GetConnectPeer",
        "networkmanager:GetCoreNetwork",
        "networkmanager:GetCoreNetworkPolicy",
```

```
        "networkmanager:GetCustomerGatewayAssociations",
        "networkmanager:GetDevices",
        "networkmanager:GetLinkAssociations",
        "networkmanager:GetLinks",
        "networkmanager:GetSites",
        "networkmanager:GetSiteToSiteVpnAttachment",
        "networkmanager:GetTransitGatewayPeering",
        "networkmanager:GetTransitGatewayRegistrations",
        "networkmanager:GetTransitGatewayRouteTableAttachment",
        "networkmanager:GetVpcAttachment",
        "networkmanager:List*",
        "nimble:GetLaunchProfile",
        "nimble:GetStreamingImage",
        "nimble:GetStudio",
        "nimble:GetStudioComponent",
        "nimble:List*",
        "oam:GetLink",
        "oam:GetSink",
        "oam:GetSinkPolicy",
        "oam:List*",
        "omics:GetAnnotationStore",
        "omics:GetReferenceStore",
        "omics:GetRunGroup",
        "omics:GetSequenceStore",
        "omics:GetVariantStore",
        "omics:GetWorkflow",
        "omics:List*",
        "opsworks-cm:Describe*",
        "opsworks-cm:List*",
        "organizations:Describe*",
        "organizations:List*",
        "osis:GetPipeline",
        "osis:List*",
        "payment-cryptography:GetAlias",
        "payment-cryptography:GetKey",
        "payment-cryptography:List*",
        "pca-connector-ad:GetConnector",
        "pca-connector-ad:GetDirectoryRegistration",
        "pca-connector-ad:GetServicePrincipalName",
        "pca-connector-ad:GetTemplate",
        "pca-connector-ad:GetTemplateGroupAccessControlEntry",
        "pca-connector-ad:List*",
        "pca-connector-scep:GetChallengeMetadata",
        "pca-connector-scep:GetConnector",
```

```
        "pca-connector-scep:List*",
        "personalize:Describe*",
        "personalize:List*",
        "pi:GetResourceMetadata",
        "pi:GetResourceMetrics",
        "pi:ListAvailableResourceDimensions",
        "pi:ListAvailableResourceMetrics",
        "pipes:Describe*",
        "pipes:List*",
        "proton:GetEnvironmentTemplate",
        "proton:GetServiceTemplate",
        "proton:List*",
        "qbusiness:GetApplication",
        "qbusiness:GetDataSource",
        "qbusiness:GetIndex",
        "qbusiness:GetPlugin",
        "qbusiness:GetRetriever",
        "qbusiness:GetWebExperience",
        "qbusiness:List*",
        "qldb:Describe*",
        "qldb:List*",
        "ram:GetPermission",
        "ram:List*",
        "rds:Describe*",
        "rds:List*",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:List*",
        "redshift:Describe*",
        "refactor-spaces:GetApplication",
        "refactor-spaces:GetEnvironment",
        "refactor-spaces:GetRoute",
        "refactor-spaces:List*",
        "rekognition:Describe*",
        "rekognition:List*",
        "resiliencehub:Describe*",
        "resiliencehub:List*",
        "resource-explorer-2:GetDefaultView",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:GetView",
        "resource-explorer-2:List*",
        "resource-groups:GetGroup",
        "resource-groups:GetGroupConfiguration",
        "resource-groups:GetGroupQuery",
```

```
        "resource-groups:GetTags",
        "resource-groups:List*",
        "robomaker:Describe*",
        "robomaker:List*",
        "route53-recovery-control-config:Describe*",
        "route53-recovery-control-config:List*",
        "route53-recovery-readiness:GetCell",
        "route53-recovery-readiness:GetReadinessCheck",
        "route53-recovery-readiness:GetRecoveryGroup",
        "route53-recovery-readiness:GetResourceSet",
        "route53-recovery-readiness:List*",
        "route53:GetDNSSEC",
        "route53:GetHealthCheck",
        "route53:GetHostedZone",
        "route53:List*",
        "route53profiles:GetProfile",
        "route53profiles:GetProfileAssociation",
        "route53profiles:GetProfileResourceAssociation",
        "route53profiles:List*",
        "route53resolver:GetFirewallDomainList",
        "route53resolver:GetFirewallRuleGroup",
        "route53resolver:GetFirewallRuleGroupAssociation",
        "route53resolver:GetOutpostResolver",
        "route53resolver:GetResolverConfig",
        "route53resolver:GetResolverQueryLogConfig",
        "route53resolver:GetResolverQueryLogConfigAssociation",
        "route53resolver:GetResolverRule",
        "route53resolver:GetResolverRuleAssociation",
        "route53resolver:List*",
        "rum:GetAppMonitor",
        "rum:List*",
        "s3-outposts:GetAccessPoint",
        "s3-outposts:GetAccessPointPolicy",
        "s3-outposts:GetBucket",
        "s3-outposts:GetBucketPolicy",
        "s3-outposts:GetBucketTagging",
        "s3-outposts:GetLifecycleConfiguration",
        "s3-outposts:List*",
        "s3:GetAccelerateConfiguration",
        "s3:GetAccessGrant",
        "s3:GetAccessGrantsInstance",
        "s3:GetAccessGrantsLocation",
        "s3:GetAccessPoint",
        "s3:GetAccessPointConfigurationForObjectLambda",
```

```
        "s3:GetAccessPointForObjectLambda",
        "s3:GetAccessPointPolicy",
        "s3:GetAccessPointPolicyForObjectLambda",
        "s3:GetAccessPointPolicyStatusForObjectLambda",
        "s3:GetAnalyticsConfiguration",
        "s3:GetBucketAcl",
        "s3:GetBucketCORS",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketMetadataTableConfiguration",
        "s3:GetBucketNotification",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketOwnershipControls",
        "s3:GetBucketPolicy",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "S3:GetBucketWebsite",
        "s3:GetEncryptionConfiguration",
        "s3:GetIntelligentTieringConfiguration",
        "s3:GetInventoryConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetMetricsConfiguration",
        "s3:GetMultiRegionAccessPoint",
        "s3:GetMultiRegionAccessPointPolicy",
        "s3:GetMultiRegionAccessPointPolicyStatus",
        "s3:GetReplicationConfiguration",
        "s3:GetStorageLensConfiguration",
        "s3:GetStorageLensConfigurationTagging",
        "s3:GetStorageLensGroup",
        "s3:List*",
        "sagemaker:Describe*",
        "sagemaker:List*",
        "scheduler:GetSchedule",
        "scheduler:GetScheduleGroup",
        "scheduler:List*",
        "schemas:Describe*",
        "schemas:GetResourcePolicy",
        "schemas:List*",
        "secretsmanager:Describe*",
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:List*",
        "securityhub:BatchGetAutomationRules",
        "securityhub:BatchGetSecurityControls",
```

```
        "securityhub:Describe*",
        "securityhub:GetConfigurationPolicy",
        "securityhub:GetConfigurationPolicyAssociation",
        "securityhub:GetEnabledStandards",
        "securityhub:GetFindingAggregator",
        "securityhub:GetInsights",
        "securityhub:List*",
        "securitylake:GetSubscriber",
        "securitylake:List*",
        "servicecatalog:Describe*",
        "servicecatalog:GetApplication",
        "servicecatalog:GetAttributeGroup",
        "servicecatalog:List*",
        "servicequotas:GetServiceQuota",
        "ses:Describe*",
        "ses:GetAccount",
        "ses:GetAddonInstance",
        "ses:GetAddonSubscription",
        "ses:GetArchive",
        "ses:GetConfigurationSet",
        "ses:GetConfigurationSetEventDestinations",
        "ses:GetContactList",
        "ses:GetDedicatedIpPool",
        "ses:GetDedicatedIps",
        "ses:GetEmailIdentity",
        "ses:GetEmailTemplate",
        "ses:GetIngressPoint",
        "ses:GetRelay",
        "ses:GetRuleSet",
        "ses:GetTemplate",
        "ses:GetTrafficPolicy",
        "ses:List*",
        "shield:Describe*",
        "shield:List*",
        "signer:GetSigningProfile",
        "signer:List*",
        "sns:GetDataProtectionPolicy",
        "sns:GetSubscriptionAttributes",
        "sns:GetTopicAttributes",
        "sns:List*",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:List*",
        "ssm-contacts:GetContact",
```

```
        "ssm-contacts:GetContactChannel",
        "ssm-contacts:List*",
        "ssm-incidents:GetReplicationSet",
        "ssm-incidents:GetResponsePlan",
        "ssm-incidents:List*",
        "ssm-sap:GetApplication",
        "ssm-sap:List*",
        "ssm:Describe*",
        "ssm:GetDefaultPatchBaseline",
        "ssm:GetDocument",
        "ssm:GetParameters",
        "ssm:GetPatchBaseline",
        "ssm:GetResourcePolicies",
        "ssm:List*",
        "sso-directory:SearchGroups",
        "sso-directory:SearchUsers",
        "sso:GetInlinePolicyForPermissionSet",
        "sso:GetManagedApplicationInstance",
        "sso:GetPermissionsBoundaryForPermissionSet",
        "sso:GetSharedSsoConfiguration",
        "sso:ListAccountAssignments",
        "sso:ListApplicationAssignments",
        "sso:ListApplications",
        "sso:ListCustomerManagedPolicyReferencesInPermissionSet",
        "sso:ListInstances",
        "sso:ListManagedPoliciesInPermissionSet",
        "sso:ListTagsForResource",
        "states:GetExecutionHistory",
        "states:Describe*",
        "states:List*",
        "synthetics:Describe*",
        "synthetics:GetCanary",
        "synthetics:GetGroup",
        "synthetics:List*",
        "tag:GetResources",
        "timestream:Describe*",
        "timestream:List*",
        "transfer:Describe*",
        "transfer:List*",
        "verifiedpermissions:GetIdentitySource",
        "verifiedpermissions:GetPolicy",
        "verifiedpermissions:GetPolicyStore",
        "verifiedpermissions:GetPolicyTemplate",
        "verifiedpermissions:GetSchema",
```

```
        "verifiedpermissions:List*",
        "vpc-lattice:GetAccessLogSubscription",
        "vpc-lattice:GetAuthPolicy",
        "vpc-lattice:GetListener",
        "vpc-lattice:GetResourcePolicy",
        "vpc-lattice:GetRule",
        "vpc-lattice:GetService",
        "vpc-lattice:GetServiceNetwork",
        "vpc-lattice:GetServiceNetworkServiceAssociation",
        "vpc-lattice:GetServiceNetworkVpcAssociation",
        "vpc-lattice:GetTargetGroup",
        "vpc-lattice:List*",
        "wafv2:GetIPSet",
        "wafv2:GetLoggingConfiguration",
        "wafv2:GetRegexPatternSet",
        "wafv2:GetRuleGroup",
        "wafv2:GetWebACL",
        "wafv2:GetWebACLForResource",
        "wafv2:List*",
        "workspaces-web:GetBrowserSettings",
        "workspaces-web:GetIdentityProvider",
        "workspaces-web:GetNetworkSettings",
        "workspaces-web:GetPortal",
        "workspaces-web:GetPortalServiceProviderMetadata",
        "workspaces-web:GetTrustStore",
        "workspaces-web:GetUserAccessLoggingSettings",
        "workspaces-web:GetUserSettings",
        "workspaces-web:List*",
        "workspaces:Describe*",
        "xray:BatchGetTraces",
        "xray:GetGroup",
        "xray:GetGroups",
        "xray:GetSamplingRules",
        "xray:GetServiceGraph",
        "xray:GetTraceSummaries",
        "xray:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AIOPSS3AccessForAmplify",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
```

```
        "s3:GetObjectVersion",
        "s3:GetObjectAcl"
      ],
      "Resource" : [
        "arn:aws:s3:::amplify",
        "arn:aws:s3:::cdk--assets--*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ViaAWSService" : [
            "amplify.amazonaws.com"
          ],
          "aws:PrincipalAccount" : [
            "${aws:ResourceAccount}"
          ]
        }
      }
    },
    {
      "Sid" : "AIOPSAPIGatewayAccess",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/restapis/*/deployments",
        "arn:aws:apigateway:*::/restapis/*/deployments/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integrations",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integrations/*",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/apis/*/deployments",
        "arn:aws:apigateway:*::/apis/*/deployments/*",
        "arn:aws:apigateway:*::/apis/*/integrations",
        "arn:aws:apigateway:*::/apis/*/integrations/*",
        "arn:aws:apigateway:*::/apis/*/stages",
        "arn:aws:apigateway:*::/apis/*/stages/*",
        "arn:aws:apigateway:*::/domainnames/*"
      ]
    }
```

```
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AIOpsConsoleAdminPolicy

説明: AWS コンソール経由で Amazon AI Operations サービスとその必要なアクセス許可へのフルアクセスを許可します。これには ID 対応コンソールセッションを使用するアクセス許可も含まれます。

`AIOpsConsoleAdminPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AIOpsConsoleAdminPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 12 月 2 日 23:51 UTC
- 編集日時: 2025 年 11 月 17 日 23:04 UTC
- ARN: `arn:aws:iam::aws:policy/AIOpsConsoleAdminPolicy`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AIOpsAdmin",
      "Effect" : "Allow",
      "Action" : [
        "aiops:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSOApplicationManagement",
      "Effect" : "Allow",
      "Action" : [
        "sso:PutApplicationAccessScope",
        "sso:PutApplicationAssignmentConfiguration",
        "sso:PutApplicationGrant",
        "sso:PutApplicationAuthenticationMethod",
        "sso:DeleteApplication"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "aiops.amazonaws.com",
          "aws:ResourceTag/ManagedByAmazonAIOperations" : "true"
        }
      }
    },
    {
      "Sid" : "SSOApplicationTagManagement",
      "Effect" : "Allow",
```

```
      "Action" : [
        "sso:CreateApplication",
        "sso:TagResource"
      ],
      "Resource" : [
        "arn:aws:sso:::instance/*",
        "arn:aws:sso::aws:applicationProvider/aiops"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "aiops.amazonaws.com",
          "aws:RequestTag/ManagedByAmazonAIOperations" : "true"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "ManagedByAmazonAIOperations"
          ]
        }
      }
    },
    {
      "Sid" : "SSOTagManagement",
      "Effect" : "Allow",
      "Action" : [
        "sso:TagResource"
      ],
      "Resource" : "arn:aws:sso::*:application/*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "aiops.amazonaws.com",
          "aws:ResourceTag/ManagedByAmazonAIOperations" : "true"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "ManagedByAmazonAIOperations"
          ]
        }
      }
    },
    {
      "Sid" : "SSOManagementAccess",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeUser",
```

```
        "sso:ListApplications",
        "sso:ListInstances",
        "sso:DescribeRegisteredRegions",
        "sso:GetSharedSsoConfiguration",
        "sso:DescribeInstance",
        "sso:GetSSOStatus",
        "sso-directory:DescribeUsers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSTSContextSetting",
      "Effect" : "Allow",
      "Action" : [
        "sts:SetContext"
      ],
      "Resource" : "arn:aws:sts::*:self"
    },
    {
      "Sid" : "IdentityPropagationAccess",
      "Effect" : "Allow",
      "Action" : [
        "signin:ListTrustedIdentityPropagationApplicationsForConsole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudtrailAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:ListTrails",
        "cloudtrail:DescribeTrails",
        "cloudtrail:ListEventDataStores"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "SSMIntegrationSecretsManagerAccess",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:PutResourcePolicy",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DeleteSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:aws/ssm/3p/*"
    },
    {
      "Sid" : "SSMIntegrationAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetServiceSetting",
        "ssm:UpdateServiceSetting"
      ],
      "Resource" : "arn:aws:ssm:*:*:servicesetting/integrations/*"
    },
    {
      "Sid" : "SSMIntegrationCreatePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreatePolicy"
      ],
      "Resource" : "arn:aws:iam::*:policy/service-role/
AWSServiceRoleSSMIntegrationsPolicy*"
    },
    {
      "Sid" : "ChatbotConfigurations",
      "Effect" : "Allow",
      "Action" : [
        "chatbot:DescribeChimeWebhookConfigurations",
        "chatbot:DescribeSlackWorkspaces",
        "chatbot:DescribeSlackChannelConfigurations",
        "chatbot:ListMicrosoftTeamsChannelConfigurations",
        "chatbot:ListMicrosoftTeamsConfiguredTeams"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMPassRoleToAIOps",
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "aiops.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMListRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TagBoundaryPermission",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetTagKeys"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMPassRoleToSSMIntegration",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.integrations.amazonaws.com"
        },
        "ArnEquals" : {
          "iam:AssociatedResourceArn" : "arn:aws:aiops:*:*:investigation-group/*"
        }
      }
    },
    {
      "Sid" : "SSMOpsItemAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateOpsItem",
        "ssm:AddTagsToResource"
      ],
      "Resource" : "arn:*:ssm:*:*:opsitem/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/Integration" : "CloudWatch",
          "aws:ResourceTag/Integration" : "CloudWatch"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Integration"
          ]
        }
      }
    },
    {
      "Sid" : "CreateAIOpsCrossAccountAssistantPolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreatePolicy"
      ],
      "Resource" : "arn:aws:iam::*:policy/AIOpsCrossAccountAssistantPolicy*"
    },
    {
      "Sid" : "AmazonQAccess",
      "Effect" : "Allow",
      "Action" : [
        "q:StartConversation",
        "q:SendMessage",
        "q:GetConversation",
        "q:ListConversations",
        "q:UpdateConversation",
        "q:DeleteConversation",
        "q:PassRequest"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AIOpsOperatorAccess

説明: 調査、調査イベント、調査リソースを作成、更新、削除するための Amazon AI Operations API へのアクセスを許可します。これには、すべての AI Operations API への読み取り専用アクセスと、ID 対応セッションの使用も含まれます。

`AIOpsOperatorAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AIOpsOperatorAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 12 月 2 日 23:51 UTC
- 編集日時: 2025 年 11 月 7 日 22:49 UTC
- ARN: `arn:aws:iam::aws:policy/AIOpsOperatorAccess`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AIOpsOperatorAccess",
      "Effect" : "Allow",
      "Action" : [
        "aiops:CreateInvestigation",
        "aiops:CreateInvestigationEvent",
        "aiops:CreateInvestigationResource",
        "aiops:DeleteInvestigation",
        "aiops:Get*",
        "aiops:List*",
        "aiops:UpdateInvestigation",
        "aiops:UpdateInvestigationEvent",
        "aiops:ValidateInvestigationGroup",
        "aiops:PutFact",
        "aiops:UpdateReport",
        "aiops:GenerateReport",
        "aiops:CreateReport",
        "q:StartConversation",
        "q:SendMessage",
        "q:GetConversation",
        "q:ListConversations",
        "q:UpdateConversation",
        "q:DeleteConversation",
        "q:PassRequest"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSOManagementAccess",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeUser",
        "sso:DescribeInstance",
        "sso-directory:DescribeUsers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSTSContextSetting",
      "Effect" : "Allow",
      "Action" : [
        "sts:SetContext"
```

```
      ],
      "Resource" : "arn:aws:sts::*:self"
    },
    {
      "Sid" : "SSMSettingServiceIntegration",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetServiceSetting"
      ],
      "Resource" : "arn:aws:ssm:*:*:servicesetting/integrations/*"
    },
    {
      "Sid" : "SSMIntegrationTagAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource",
        "ssm:CreateOpsItem"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/Integration" : [
            "CloudWatch"
          ]
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "Integration"
        }
      }
    },
    {
      "Sid" : "SSMOpsItemIntegration",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteOpsItem",
        "ssm:UpdateOpsItem"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/Integration" : [
            "CloudWatch"
          ]
        }
```

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AIOpsReadOnlyAccess

説明: Amazon AI Operations サービスとその必要なリソースに ReadOnly アクセス許可を付与します。

`AIOpsReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AIOpsReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 12 月 2 日 23:51 UTC
- 編集日時: 2025 年 6 月 24 日 00:22 UTC
- ARN: `arn:aws:iam::aws:policy/AIOpsReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AIOpsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "aiops:Get*",
        "aiops:List*",
        "aiops:ValidateInvestigationGroup"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "SSOManagementAccess",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeUser",
        "sso:DescribeInstance",
        "sso-directory:DescribeUsers"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AlexaForBusinessDeviceSetup

説明: AlexaForBusiness サービスへのデバイスセットアップアクセスを提供します

`AlexaForBusinessDeviceSetup` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AlexaForBusinessDeviceSetup` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 11 月 30 日 16:47 UTC
- 編集日時: 2019 年 5 月 20 日 21:05 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessDeviceSetup`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AlexaForBusinessFullAccess

説明: AlexaForBusiness リソースへのフルアクセスと、関連する へのアクセスを許可します AWS のサービス

AlexaForBusinessFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AlexaForBusinessFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 11 月 30 日 16:47 UTC
- 編集日時: 2020 年 7 月 1 日 21:01 UTC
- ARN: arn:aws:iam::aws:policy/AlexaForBusinessFullAccess

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AlexaForBusinessGatewayExecution

説明: AlexaForBusiness サービスへのゲートウェイ実行アクセスを提供します

`AlexaForBusinessGatewayExecution` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AlexaForBusinessGatewayExecution` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 11 月 30 日 16:47 UTC
- 編集日時: 2017 年 11 月 30 日 16:47 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessGatewayExecution`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AlexaForBusinessLifesizeDelegatedAccessPolicy

説明: Lifesize AVS デバイスへのアクセスを提供します

AlexaForBusinessLifesizeDelegatedAccessPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AlexaForBusinessLifesizeDelegatedAccessPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 6 月 4 日 19:46 UTC
- 編集日時: 2020 年 6 月 12 日 20:31 UTC
- ARN: arn:aws:iam::aws:policy/AlexaForBusinessLifesizeDelegatedAccessPolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AlexaForBusinessNetworkProfileServicePolicy

説明: このポリシーにより、ネットワークプロファイルによってスケジュールされた自動タスクを Alexa for Business が実行できるようになります。

`AlexaForBusinessNetworkProfileServicePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 3 月 13 日 00:53 UTC
- 編集日時: 2019 年 4 月 5 日 21:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AlexaForBusinessNetworkProfileServicePolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AlexaForBusinessPolyDelegatedAccessPolicy

説明: Poly AVS デバイスへのアクセスを提供します

`AlexaForBusinessPolyDelegatedAccessPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AlexaForBusinessPolyDelegatedAccessPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 10 月 16 日 19:48 UTC
- 編集日時: 2019 年 10 月 16 日 19:48 UTC
- ARN: arn:aws:iam::aws:policy/AlexaForBusinessPolyDelegatedAccessPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AlexaForBusinessReadOnlyAccess

説明: AlexaForBusiness サービスへの読み取り専用アクセスを提供します

`AlexaForBusinessReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AlexaForBusinessReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 11 月 30 日 16:47 UTC
- 編集日時: 2019 年 11 月 20 日 00:25 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonAPIGatewayAdministrator

説明: AWS マネジメントコンソールを使用して Amazon API Gateway で API を作成/編集/削除するためのフルアクセスを提供します。

`AmazonAPIGatewayAdministrator` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonAPIGatewayAdministrator` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 7 月 9 日 17:34 UTC
- 編集日時: 2015 年 7 月 9 日 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAPIGatewayAdministrator`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonAPIGatewayInvokeFullAccess

説明: Amazon API Gateway で API を呼び出すためのフルアクセスを提供します。

AmazonAPIGatewayInvokeFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonAPIGatewayInvokeFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 7 月 9 日 17:36 UTC
- 編集日時: 2018 年 12 月 18 日 18:25 UTC
- ARN: arn:aws:iam::aws:policy/AmazonAPIGatewayInvokeFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonAPIGatewayPushToCloudWatchLogs

説明: API Gateway がユーザーのアカウントにログをプッシュできるようにします。

AmazonAPIGatewayPushToCloudWatchLogs は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonAPIGatewayPushToCloudWatchLogs をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 11 月 11 日 23:41 UTC
- 編集日時: 2015 年 11 月 11 日 23:41 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonAPIGatewayPushToCloudWatchLogs

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonAppFlowFullAccess

説明: Amazon AppFlow へのフルアクセスと、フローソースまたは送信先 (S3 および Redshift) としてサポートされている AWS サービスへのアクセスを提供します。また、KMS にアクセスして暗号化することもできます。

`AmazonAppFlowFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonAppFlowFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 6 月 2 日 23:30 UTC
- 編集日時: 2022 年 2 月 28 日 23:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAppFlowFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonAppFlowReadOnlyAccess

説明: Amazon Appflow フローへの読み取り専用アクセスを提供します

`AmazonAppFlowReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonAppFlowReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 6 月 2 日 23:26 UTC
- 編集日時: 2022 年 2 月 28 日 20:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAppFlowReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonApplicationRecoveryControllerRegionSwitchPlanExecutionPolicy

説明: 計画実行と計画評価のためのアクセス許可を ARC リージョンスイッチに付与します。

AmazonApplicationRecoveryControllerRegionSwitchPlanExecutionPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonApplicationRecoveryControllerRegionSwitchPlanExecutionPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 11 月 3 日 19:34 UTC
- 編集日時: 2025 年 11 月 3 日 19:34 UTC
- ARN: arn:aws:iam::aws:policy/AmazonApplicationRecoveryControllerRegionSwitchPlanExecutionPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonAppStreamFullAccess

説明: 経由で Amazon AppStream へのフルアクセスを提供します AWS マネジメントコンソール。

`AmazonAppStreamFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonAppStreamFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2020 年 8 月 28 日 17:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAppStreamFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonAppStreamPCAAccess

説明: Amazon AppStream 2.0 での証明書ベースの認証のためのカスタマーアカウントの AWS Certificate Manager Private CA へのアクセス

`AmazonAppStreamPCAAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonAppStreamPCAAccess` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 10 月 24 日 17:05 UTC
- 編集日時: 2022 年 10 月 24 日 17:05 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonAppStreamPCAAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
```

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonAppStreamReadOnlyAccess

説明: 経由で Amazon AppStream への読み取り専用アクセスを提供します AWS マネジメントコンソール。

`AmazonAppStreamReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonAppStreamReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2025 年 10 月 22 日 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAppStreamReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonAppStreamServiceAccess

説明: Amazon AppStream サービスロールのデフォルトポリシー。

AmazonAppStreamServiceAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonAppStreamServiceAccess をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2016 年 11 月 19 日 04:17 UTC
- 編集日時: 2025 年 11 月 17 日 18:19 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonAppStreamServiceAccess

ポリシーのバージョン

ポリシーのバージョン: v9 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeImages",
        "ec2:DescribeAvailabilityZones",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeSubnets",
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
```

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonAthenaFullAccess

説明: Amazon Athena へのフルアクセスと、クエリ、結果の書き込み、データ管理に必要な依存関係へのスコープ付きアクセスを提供します。

AmazonAthenaFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonAthenaFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2016 年 11 月 30 日 16:46 UTC
- 編集日時: 2025 年 1 月 3 日 00:37 UTC
- ARN: arn:aws:iam::aws:policy/AmazonAthenaFullAccess

ポリシーのバージョン

ポリシーのバージョン: v13 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

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

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

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonAthenaServiceRolePolicy

説明: Amazon Athena の実行に必要な他の AWS サービスリソースへのアクセスを許可します

AmazonAthenaServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2025 年 11 月 14 日 22:34 UTC
- 編集日時: 2025 年 11 月 14 日 22:34 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonAthenaServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonAugmentedAIFullAccess

説明: FlowDefinition、HumanTaskUi、HumanLoop など、Amazon Augmented AI リソースのすべてのオペレーションを実行するためのアクセスを提供します。一般公開のワークチームに対する FlowDefinition の作成にはアクセスできません。

`AmazonAugmentedAIFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonAugmentedAIFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 12 月 3 日 16:21 UTC
- 編集日時: 2019 年 12 月 3 日 16:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAugmentedAIFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonAugmentedAIHumanLoopFullAccess

説明: HumanLoops のすべてのオペレーションを実行するためのアクセスを提供します。

AmazonAugmentedAIHumanLoopFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonAugmentedAIHumanLoopFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 12 月 3 日 16:20 UTC

- 編集日時: 2019 年 12 月 3 日 16:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAugmentedAIHumanLoopFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonAugmentedAIIntegratedAPIAccess

説明: FlowDefinition、HumanTaskUi、HumanLoop など、Amazon Augmented AI リソースのすべてのオペレーションを実行するためのアクセスを提供します。また、Amazon Augmented AI と統合されたサービスの運用にもアクセスできます。

AmazonAugmentedAIIntegratedAPIAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonAugmentedAIIntegratedAPIAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 4 月 22 日 20:47 UTC
- 編集日時: 2020 年 4 月 22 日 20:47 UTC
- ARN: arn:aws:iam::aws:policy/AmazonAugmentedAIIntegratedAPIAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonAuroraDSQLConsoleFullAccess

説明: Aurora DSQL へのコンソールフル管理アクセスを提供します

`AmazonAuroraDSQLConsoleFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonAuroraDSQLConsoleFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 12 月 3 日 15:36 UTC
- 編集日時: 2025 年 10 月 23 日 17:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAuroraDSQLConsoleFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
  "Statement" : [
    {
      "Sid" : "DsqlAllPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dsql:PutClusterPolicy",
        "dsql:GetClusterPolicy",
        "dsql:DeleteClusterPolicy",
        "dsql:CreateCluster",
        "dsql:GetCluster",
        "dsql:UpdateCluster",
        "dsql:DeleteCluster",
        "dsql:ListClusters",
        "dsql:TagResource",
        "dsql:UntagResource",
        "dsql:ListTagsForResource",
        "dsql:DbConnectAdmin",
        "dsql:DbConnect",
        "dsql:PutMultiRegionProperties",
        "dsql:PutWitnessRegion",
        "dsql:AddPeerCluster",
        "dsql:RemovePeerCluster",
        "dsql:GetVpcEndpointServiceName",
        "dsql:StartBackupJob",
        "dsql:GetBackupJob",
        "dsql:StopBackupJob",
        "dsql:StartRestoreJob",
        "dsql:GetRestoreJob",
        "dsql:StopRestoreJob",
        "dsql:InjectError"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DsqlConsolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:ValidatePolicy",
        "tag:GetTagKeys",
        "tag:GetTagValues",
        "cloudwatch:GetMetricData",
        "ec2:DescribeVpcEndpoints",
        "kms:ListAliases",
        "kms:DescribeKey"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSCryptographicPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "dsql.*.amazonaws.com"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:dsql:ClusterId"
        }
      }
    },
    {
      "Sid" : "CreateDsqlServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "dsql.amazonaws.com"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonAuroraDSQLFullAccess

説明: Aurora DSQL へのフル管理アクセスを提供します

AmazonAuroraDSQLFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonAuroraDSQLFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 12 月 3 日 15:36 UTC
- 編集日時: 2025 年 10 月 23 日 18:04 UTC
- ARN: arn:aws:iam::aws:policy/AmazonAuroraDSQLFullAccess

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DsqlAllPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dsql:PutClusterPolicy",
        "dsql:GetClusterPolicy",
```

```
        "dsql:DeleteClusterPolicy",
        "dsql:CreateCluster",
        "dsql:GetCluster",
        "dsql:UpdateCluster",
        "dsql:DeleteCluster",
        "dsql:ListClusters",
        "dsql:TagResource",
        "dsql:UntagResource",
        "dsql:ListTagsForResource",
        "dsql:DbConnectAdmin",
        "dsql:DbConnect",
        "dsql:PutMultiRegionProperties",
        "dsql:PutWitnessRegion",
        "dsql:AddPeerCluster",
        "dsql:RemovePeerCluster",
        "dsql:GetVpcEndpointServiceName",
        "dsql:StartBackupJob",
        "dsql:GetBackupJob",
        "dsql:StopBackupJob",
        "dsql:StartRestoreJob",
        "dsql:GetRestoreJob",
        "dsql:StopRestoreJob",
        "dsql:InjectError"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RelatedServicesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateDsqlServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "dsql.amazonaws.com"
        }
      }
```

```
    },
    {
      "Sid" : "KMSDescribePermission",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "dsql.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "KMSCryptographicPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "dsql.*.amazonaws.com"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:dsql:ClusterId"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonAuroraDSQLReadOnlyAccess

説明: Aurora DSQL への読み取り専用アクセスを提供します

`AmazonAuroraDSQLReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonAuroraDSQLReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 12 月 3 日 15:21 UTC
- 編集日時: 2025 年 10 月 23 日 17:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAuroraDSQLReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
```

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonBedrockAgentCoreMemoryBedrockModelInferenceExecutionRo

説明: Bedrock エージェントコアメモリへの Bedrock モデル推論を実行できるようにするアクセス許可を提供します

AmazonBedrockAgentCoreMemoryBedrockModelInferenceExecutionRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonBedrockAgentCoreMemoryBedrockModelInferenceExecutionRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 7 月 16 日 13:37 UTC
- 編集日時: 2025 年 7 月 16 日 13:37 UTC
- ARN: arn:aws:iam::aws:policy/AmazonBedrockAgentCoreMemoryBedrockModelInferenceExecutionRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*",
        "arn:aws:bedrock:*:*:inference-profile/*"
      ],
      "Condition" : {
```

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonBedrockFullAccess

説明: Amazon Bedrock へのフルアクセスと、Amazon Bedrock が必要とする関連サービスへの制限付きアクセスを提供します

`AmazonBedrockFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonBedrockFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 12 月 6 日 15:47 UTC
- 編集日時: 2025 年 12 月 5 日 05:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockAll",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BedrockMantleAll",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-mantle:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeKey",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:*:kms:*:::*"
    },
    {
      "Sid" : "APIsWithAllResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
```

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

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

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

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

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonBedrockLimitedAccess

説明: Amazon Bedrock と、Amazon Bedrock が必要とする関連サービスへの制限付きアクセスを提供します

`AmazonBedrockLimitedAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonBedrockLimitedAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 6 月 29 日 22:22 UTC
- 編集日時: 2025 年 12 月 5 日 05:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockLimitedAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeKey",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:*:kms:*:::*"
    },
    {
      "Sid" : "APIsWithAllResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BedrockMantleAPIs",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-mantle:CallWithBearerToken",
        "bedrock-mantle:Get*",
        "bedrock-mantle:List*",
        "bedrock-mantle:CreateInference"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MarketplaceOperationsFromBedrockFor3pModels",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:Subscribe",
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:CalledViaLast" : "bedrock.amazonaws.com"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonBedrockMantleFullAccess

説明: Amazon Bedrock Mantle へのフルアクセスと、Amazon Bedrock Mantle に必要な関連サービスへの制限付きアクセスを提供します

`AmazonBedrockMantleFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonBedrockMantleFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 12 月 4 日 07:19 UTC
- 編集日時: 2025 年 12 月 4 日 07:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockMantleFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonBedrockMantleInferenceAccess

説明: Amazon Bedrock Mantle への読み取りおよび推論作成アクセスを提供します

`AmazonBedrockMantleInferenceAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonBedrockMantleInferenceAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 12 月 4 日 07:19 UTC
- 編集日時: 2025 年 12 月 4 日 07:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockMantleInferenceAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonBedrockMantleReadOnly

説明: Amazon Bedrock Mantle への読み取り専用アクセスを提供します

`AmazonBedrockMantleReadOnly` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonBedrockMantleReadOnly` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 12 月 4 日 07:19 UTC
- 編集日時: 2025 年 12 月 4 日 07:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockMantleReadOnly`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonBedrockMarketplaceAccess

説明: Amazon Bedrock Marketplace と、Amazon Bedrock Marketplace が必要とする関連サービスへの制限付きアクセスを提供します

`AmazonBedrockMarketplaceAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonBedrockMarketplaceAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2025 年 6 月 29 日 22:22 UTC
- 編集日時: 2025 年 6 月 29 日 22:22 UTC
- ARN: arn:aws:iam::aws:policy/AmazonBedrockMarketplaceAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockMarketplaceAPIs",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateMarketplaceModelEndpoint",
        "bedrock:DeleteMarketplaceModelEndpoint",
        "bedrock:DeregisterMarketplaceModelEndpoint",
        "bedrock:RegisterMarketplaceModelEndpoint",
        "bedrock:UpdateMarketplaceModelEndpoint"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MarketplaceModelEndpointMutatingAPIs",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateModel",
        "sagemaker:DeleteEndpoint",
        "sagemaker:UpdateEndpoint"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*",
```

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

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

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

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonBedrockReadOnly

説明: Amazon Bedrock への読み取り専用アクセスを提供します

AmazonBedrockReadOnly は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonBedrockReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 12 月 6 日 15:48 UTC
- 編集日時: 2024 年 12 月 4 日 19:36 UTC
- ARN: arn:aws:iam::aws:policy/AmazonBedrockReadOnly

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonBedrockReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:Get*",
        "bedrock:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MarketplaceModelEndpointNonMutatingAPIs",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeModel",
```

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonBedrockStudioPermissionsBoundary

説明: Amazon Bedrock Studio が Amazon Bedrock Studio リソースを操作するために作成する IAM ロールの最大アクセス許可を定義します。

AmazonBedrockStudioPermissionsBoundary は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonBedrockStudioPermissionsBoundary をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 8 月 1 日 00:24 UTC
- 編集日時: 2024 年 8 月 1 日 00:24 UTC
- ARN: arn:aws:iam::aws:policy/AmazonBedrockStudioPermissionsBoundary

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AccessS3Buckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
```

```
        "s3:ListBucketVersions",
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:GetObjectVersion",
        "s3:DeleteObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::br-studio-${aws:PrincipalAccount}-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AccessOpenSearchCollections",
      "Effect" : "Allow",
      "Action" : "aoss:APIAccessAll",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "InvokeBedrockModels",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : "arn:aws:bedrock:*::foundation-model/*"
    },
    {
      "Sid" : "AccessBedrockResources",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeAgent",
        "bedrock:Retrieve",
        "bedrock:StartIngestionJob",
        "bedrock:GetIngestionJob",
        "bedrock:ListIngestionJobs",
        "bedrock:ApplyGuardrail",
```

```
        "bedrock:ListPrompts",
        "bedrock:GetPrompt",
        "bedrock:CreatePrompt",
        "bedrock:DeletePrompt",
        "bedrock:CreatePromptVersion",
        "bedrock:InvokeFlow",
        "bedrock:ListTagsForResource",
        "bedrock:TagResource",
        "bedrock:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonBedrockManaged" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "RetrieveAndGenerate",
      "Effect" : "Allow",
      "Action" : "bedrock:RetrieveAndGenerate",
      "Resource" : "*"
    },
    {
      "Sid" : "WriteLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/lambda/br-studio-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonBedrockManaged" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
```

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

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonBraketFullAccess

説明: AWS マネジメントコンソール および SDK 経由で Amazon Braket へのフルアクセスを提供します。関連サービス (S3、ログなど) へのアクセスも提供します。

AmazonBraketFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonBraketFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 8 月 6 日 20:12 UTC
- 編集日時: 2025 年 4 月 11 日 22:22 UTC
- ARN: arn:aws:iam::aws:policy/AmazonBraketFullAccess

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:ListBucket",
        "s3:CreateBucket",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketPolicy"
```

```
      ],
      "Resource" : "arn:aws:s3:::amazon-braket-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "servicequotas:GetServiceQuota",
        "cloudwatch:GetMetricData",
        "pricing:GetProducts"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "ecr:BatchCheckLayerAvailability"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/amazon-braket*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:Describe*",
        "logs:Get*",
        "logs:List*",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:TestMetricFilter",
        "logs:FilterLogEvents"
```

```
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/braket*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "iam:ListRolePolicies",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListNotebookInstances"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreatePresignedNotebookInstanceUrl",
        "sagemaker:CreateNotebookInstance",
        "sagemaker:DeleteNotebookInstance",
        "sagemaker:DescribeNotebookInstance",
        "sagemaker:StartNotebookInstance",
        "sagemaker:StopNotebookInstance",
        "sagemaker:UpdateNotebookInstance",
        "sagemaker:ListTags",
        "sagemaker:AddTags",
        "sagemaker:DeleteTags"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:notebook-instance/amazon-braket-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeNotebookInstanceLifecycleConfig",
        "sagemaker:CreateNotebookInstanceLifecycleConfig",
        "sagemaker:DeleteNotebookInstanceLifecycleConfig",
        "sagemaker:ListNotebookInstanceLifecycleConfigs",
```

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

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonBraketJobsExecutionPolicy

説明: S3 AWS のサービス 、Cloudwatch、IAM、Braket などの Amazon Braket ジョブの実行に必要な および リソースへのアクセスを許可します。

AmazonBraketJobsExecutionPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonBraketJobsExecutionPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 11 月 26 日 19:34 UTC
- 編集日時: 2021 年 11 月 28 日 05:34 UTC
- ARN: arn:aws:iam::aws:policy/AmazonBraketJobsExecutionPolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonBraketServiceRolePolicy

説明: Amazon Braket がユーザーに代わって AWS リソースを作成および管理することを許可する

AmazonBraketServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 8 月 4 日 17:12 UTC
- 編集日時: 2025 年 7 月 11 日 21:37 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonBraketServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonChimeFullAccess

説明: AWS マネジメントコンソール経由で Amazon Chime 管理者コンソールへのフルアクセスを提供します。

AmazonChimeFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonChimeFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 11 月 1 日 22:15 UTC
- 編集日時: 2020 年 12 月 14 日 21:00 UTC
- ARN: arn:aws:iam::aws:policy/AmazonChimeFullAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonChimeReadOnly

説明: AWS マネジメントコンソール経由で Amazon Chime 管理者コンソールへの読み取り専用アクセスを提供します。

`AmazonChimeReadOnly` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonChimeReadOnly` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 11 月 1 日 22:04 UTC
- 編集日時: 2020 年 12 月 14 日 20:53 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonChimeReadOnly`

ポリシーのバージョン

ポリシーのバージョン: v10 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonChimeSDK

説明: Amazon Chime SDK オペレーションへのアクセスを提供します

AmazonChimeSDK は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonChimeSDK をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 2 月 4 日 21:53 UTC
- 編集日時: 2023 年 1 月 10 日 18:05 UTC
- ARN: arn:aws:iam::aws:policy/AmazonChimeSDK

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy

説明: Amazon Chime SDK MediaPipelines サービスリンクロール向けマネージドポリシー

AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 4 月 4 日 22:02 UTC
- 編集日時: 2023 年 12 月 8 日 19:14 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonChimeSDKMessagingServiceRolePolicy

説明: Amazon Chime SDK Messaging が AWS リソースにアクセスし、メッセージング機能を有効にすることを許可する

AmazonChimeSDKMessagingServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 3 月 3 日 01:43 UTC

- 編集日時: 2023 年 3 月 3 日 01:43 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonChimeSDKMessagingServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonChimeServiceRolePolicy

説明: Amazon Chime が使用または管理する AWS リソースへのアクセスを有効にします

AmazonChimeServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 9 月 30 日 22:25 UTC
- 編集日時: 2019 年 9 月 30 日 22:25 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonChimeServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonChimeTranscriptionServiceLinkedRolePolicy

説明: Amazon Chime がユーザーに代わって Amazon Transcribe および Amazon Transcribe Medical にアクセスすることを許可します

AmazonChimeTranscriptionServiceLinkedRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 8 月 4 日 21:47 UTC
- 編集日時: 2021 年 8 月 4 日 21:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeTranscriptionServiceLinkedRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonChimeUserManagement

説明: AWS マネジメントコンソール経由で Amazon Chime 管理者コンソールへのユーザー管理アクセスを提供します。

AmazonChimeUserManagement は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonChimeUserManagement をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 11 月 1 日 22:17 UTC
- 編集日時: 2020 年 2 月 18 日 19:26 UTC
- ARN: arn:aws:iam::aws:policy/AmazonChimeUserManagement

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonChimeVoiceConnectorServiceLinkedRolePolicy

説明: Amazon Chime VoiceConnector のサービスリンクロール向けマネージドポリシー

AmazonChimeVoiceConnectorServiceLinkedRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 9 月 30 日 22:16 UTC
- 編集日時: 2023 年 4 月 14 日 21:49 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonChimeVoiceConnectorServiceLinkedRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonCloudDirectoryFullAccess

説明: Amazon Cloud Directory サービスへのフルアクセスを提供します。

`AmazonCloudDirectoryFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonCloudDirectoryFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 2 月 25 日 00:41 UTC
- 編集日時: 2017 年 2 月 25 日 00:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudDirectoryFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonCloudDirectoryReadOnlyAccess

説明: Amazon Cloud Directory サービスへの読み取り専用アクセスを提供します。

AmazonCloudDirectoryReadOnlyAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonCloudDirectoryReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 2 月 28 日 23:42 UTC
- 編集日時: 2017 年 2 月 28 日 23:42 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCloudDirectoryReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonCloudWatchEvidentlyFullAccess

説明: Amazon CloudWatch Evidently へのフルアクセスのみを提供します。関連する Amazon S3、Amazon SNS、Amazon CloudWatch およびその他の関連サービスへのアクセスも提供されます。

`AmazonCloudWatchEvidentlyFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonCloudWatchEvidentlyFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 11 月 29 日 15:10 UTC
- 編集日時: 2021 年 11 月 29 日 15:10 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchEvidentlyFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonCloudWatchEvidentlyReadOnlyAccess

説明: Amazon CloudWatch Evidently への読み取り専用アクセスを提供します

AmazonCloudWatchEvidentlyReadOnlyAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonCloudWatchEvidentlyReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 11 月 29 日 15:08 UTC
- 編集日時: 2021 年 11 月 29 日 15:08 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchEvidentlyReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する

- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonCloudWatchEvidentlyServiceRolePolicy

説明: CloudWatch Evidently Service が顧客に代わって関連する AWS リソースを管理できるようにします

`AmazonCloudWatchEvidentlyServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 9 月 13 日 17:25 UTC
- 編集日時: 2022 年 9 月 13 日 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCloudWatchEvidentlyServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonCloudWatchRUMFullAccess

説明: Amazon CloudWatch RUM サービスへのフルアクセス権を付与

`AmazonCloudWatchRUMFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonCloudWatchRUMFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 11 月 29 日 15:46 UTC
- 編集日時: 2021 年 11 月 29 日 15:46 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchRUMFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonCloudWatchRUMReadOnlyAccess

説明: Amazon CloudWatch RUM サービスの読み取り専用アクセス許可を付与

`AmazonCloudWatchRUMReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonCloudWatchRUMReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 11 月 29 日 15:43 UTC
- 編集日時: 2025 年 6 月 12 日 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchRUMReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "rum:GetAppMonitor",
        "rum:GetAppMonitorData",
        "rum:ListAppMonitors",
        "rum:ListRumMetricsDestinations",
        "rum:BatchGetRumMetricDefinitions",
        "rum:GetResourcePolicy",
        "rum:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "synthetics:describeCanariesLastRun",
        "synthetics:describeCanaries"
      ],
      "Resource" : "arn:aws:synthetics:*:*:canary:*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group::log-stream:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:GetTraceSummaries"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonCloudWatchRUMServiceRolePolicy

説明: Amazon CloudWatch RUM Service にモニタリングデータを他の関連 AWS サービスに発行するアクセス許可を付与します

AmazonCloudWatchRUMServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 11 月 17 日 23:17 UTC
- 編集日時: 2023 年 2 月 22 日 20:35 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonCloudWatchRUMServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonCodeCatalystFullAccess

説明: Amazon CodeCatalyst へのフルアクセスを提供します

`AmazonCodeCatalystFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonCodeCatalystFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2023 年 4 月 20 日 16:50 UTC
- 編集日時: 2023 年 4 月 20 日 16:50 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCodeCatalystFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonCodeCatalystReadOnlyAccess

説明: Amazon CodeCatalyst への読み取り専用アクセスを提供します

`AmazonCodeCatalystReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonCodeCatalystReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 4 月 20 日 16:49 UTC
- 編集日時: 2023 年 4 月 20 日 16:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeCatalystReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonCodeCatalystSupportAccess

説明: Amazon CodeCatalyst がユーザーに代わって AWS サポート ケースを作成、更新、解決できるようにします。

`AmazonCodeCatalystSupportAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonCodeCatalystSupportAccess` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 4 月 20 日 12:34 UTC

- 編集日時: 2023 年 4 月 20 日 12:34 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonCodeCatalystSupportAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonCodeGuruProfilerAgentAccess

説明: Amazon CodeGuru Profiler エージェントが必要とするアクセスを提供します。

`AmazonCodeGuruProfilerAgentAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonCodeGuruProfilerAgentAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 2 月 5 日 22:11 UTC
- 編集日時: 2022 年 5 月 5 日 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruProfilerAgentAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonCodeGuruProfilerFullAccess

説明: Amazon CodeGuru Profiler へのフルアクセスを提供します。

`AmazonCodeGuruProfilerFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonCodeGuruProfilerFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 12 月 3 日 10:13 UTC
- 編集日時: 2020 年 7 月 15 日 03:23 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruProfilerFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する

- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonCodeGuruProfilerReadOnlyAccess

説明: Amazon CodeGuru Profiler への読み取り専用アクセスを提供します。

AmazonCodeGuruProfilerReadOnlyAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonCodeGuruProfilerReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 12 月 3 日 10:30 UTC
- 編集日時: 2020 年 6 月 27 日 23:52 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCodeGuruProfilerReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonCodeGuruReviewerFullAccess

説明: Amazon CodeGuru Reviewer へのフルアクセス権と、必要な依存関係へのスコープ付きアクセス権を付与します。

`AmazonCodeGuruReviewerFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonCodeGuruReviewerFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 12 月 3 日 08:33 UTC
- 編集日時: 2020 年 8 月 29 日 04:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruReviewerFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonCodeGuruReviewerReadOnlyAccess

説明: Amazon CodeGuru Reviewer への読み取り専用アクセスを提供します。

AmazonCodeGuruReviewerReadOnlyAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonCodeGuruReviewerReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 12 月 3 日 08:48 UTC
- 編集日時: 2020 年 8 月 29 日 04:15 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCodeGuruReviewerReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonCodeGuruReviewerServiceRolePolicy

説明: Amazon CodeGuru Reviewer がユーザーに代わってリソースにアクセスするために必要なサービスリンクロールです。

`AmazonCodeGuruReviewerServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 12 月 3 日 05:31 UTC
- 編集日時: 2020 年 11 月 27 日 15:09 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCodeGuruReviewerServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonCodeGuruSecurityFullAccess

説明: Amazon CodeGuru Security へのフルアクセスを提供します。

AmazonCodeGuruSecurityFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonCodeGuruSecurityFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 5 月 9 日 21:03 UTC
- 編集日時: 2023 年 5 月 9 日 21:03 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCodeGuruSecurityFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
      "Effect" : "Allow",
      "Action" : [
        "codeguru-security:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonCodeGuruSecurityScanAccess

説明: Amazon CodeGuru Security スキャンの操作に必要なアクセスを提供します。

AmazonCodeGuruSecurityScanAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonCodeGuruSecurityScanAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 5 月 9 日 20:54 UTC
- 編集日時: 2023 年 5 月 9 日 20:54 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCodeGuruSecurityScanAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonCognitoDeveloperAuthenticatedIdentities

説明: Amazon Cognito API へのアクセスを提供して、認証バックエンドから送信される開発者認証アイデンティティをサポートします。

`AmazonCognitoDeveloperAuthenticatedIdentities` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonCognitoDeveloperAuthenticatedIdentities をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 3 月 24 日 17:22 UTC
- 編集日時: 2015 年 3 月 24 日 17:22 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCognitoDeveloperAuthenticatedIdentities

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonCognitoIdpEmailServiceRolePolicy

説明: Amazon Cognito のユーザープールサービスが SES アイデンティティを使用して E メールを送信できるようにします。

`AmazonCognitoIdpEmailServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 3 月 21 日 21:32 UTC
- 編集日時: 2019 年 3 月 21 日 21:32 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCognitoIdpEmailServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonCognitoIdpServiceRolePolicy

説明: Amazon Cognito ユーザープールが使用または管理する AWS のサービス および リソースへのアクセスを有効にします

AmazonCognitoIdpServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 6 月 26 日 22:30 UTC
- 編集日時: 2020 年 6 月 26 日 22:30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCognitoIdpServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonCognitoPowerUser

説明: 既存の Amazon Cognito リソースへの管理者アクセスを提供します。新しい Cognito AWS アカウント リソースを作成するには、管理者権限が必要です。

AmazonCognitoPowerUser は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonCognitoPowerUser をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 3 月 24 日 17:14 UTC
- 編集日時: 2025 年 2 月 27 日 18:37 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCognitoPowerUser

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonCognitoReadOnly

説明: Amazon Cognito リソースへの読み取り専用アクセスを提供します。

`AmazonCognitoReadOnly` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonCognitoReadOnly` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 3 月 24 日 17:06 UTC
- 編集日時: 2019 年 8 月 1 日 19:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoReadOnly`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonCognitoUnAuthedIdentitiesSessionPolicy

説明: このポリシーは、Cognito アイデンティティプールの未認証アイデンティティに許可される権限のセットを定義します。このポリシーは、スタンドアロンのアクセス許可ポリシーとして使用することを意図したものではありません。アイデンティティプール内のロールにアタッチされている過度に許容度の高いポリシーに対するガードレールとして使用されます。このポリシーはどのロールにもアタッチしないでください。Cognito Identity Service は、認証情報を作成するときに、このポリシーをスコープダウンポリシーとして自動的に含めます。拡張フローを通じて他の AWS リソースに一時的にアクセスする権限は、サービスによって提供される認証されていないユーザーのアイデンティ

ティに関連付けられたロールと、Cognito が所有するこの管理ポリシーで付与される権限の共通部分によって定義されるようになりました。

AmazonCognitoUnAuthedIdentitiesSessionPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonCognitoUnAuthedIdentitiesSessionPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 7 月 19 日 23:04 UTC
- 編集日時: 2024 年 11 月 1 日 18:12 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCognitoUnAuthedIdentitiesSessionPolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CognitoUnAuthedIdentitiesSessionPolicy",
      "Effect" : "Allow",
      "Action" : [
        "rum:PutRumEvents",
        "sagemaker:InvokeEndpoint",
        "polly:*",
        "comprehend:*",
        "translate:*",
        "transcribe:*",
```

```
        "rekognition:*",
        "mobiletargeting:*",
        "firehose:*",
        "personalize:*",
        "geo:GetMap*",
        "geo:SearchPlaceIndex*",
        "geo:GetPlace",
        "geo:CalculateRoute*",
        "geo:*Geofence",
        "geo:*Geofences",
        "geo:*DevicePosition*",
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyPair",
        "kms:GenerateDataKeyPairWithoutPlaintext",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonCognitoUnauthenticatedIdentities

説明: このポリシーは、Cognito アイデンティティプールの未認証アイデンティティに許可される権限のセットを定義します。これを unauth ロールにアタッチする必要はありません。Cognito Identity Service は、認証情報を作成するときに、このロールをスコープダウンポリシーとして自動的に含めます。拡張フローを通じて他の AWS リソースに一時的にアクセスする権限は、サービスによって提供される認証されていないユーザーのアイデンティティに関連付けられたロールと、Cognito が所有するこの管理ポリシーで付与される権限の共通部分によって定義されるようになりました。

AmazonCognitoUnauthenticatedIdentities は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonCognitoUnauthenticatedIdentities をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 2 月 1 日 22:36 UTC
- 編集日時: 2023 年 2 月 1 日 22:36 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCognitoUnauthenticatedIdentities

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonConnect_FullAccess

説明: このポリシーの目的は、 AWS Connect リソースの使用に必要なアクセス許可を Connect ユーザーに付与することです。このポリシーは、 AWS Connect コンソールとパブリック APIs

AmazonConnect_FullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonConnect_FullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 11 月 20 日 19:54 UTC
- 編集日時: 2023 年 3 月 7 日 14:49 UTC
- ARN: arn:aws:iam::aws:policy/AmazonConnect_FullAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonConnectCampaignsServiceLinkedRolePolicy

説明: Amazon Connect Campaigns サービスリンクロールのポリシー

`AmazonConnectCampaignsServiceLinkedRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 9 月 23 日 20:54 UTC
- 編集日時: 2024 年 10 月 3 日 20:20 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ConnectCampaignAccess",
      "Effect" : "Allow",
      "Action" : [
        "connect-campaigns:ListCampaigns"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConnectAccess",
      "Effect" : "Allow",
      "Action" : [
        "connect:BatchPutContact",
        "connect:StopContact",
        "connect:DescribeContactFlow",
        "connect:SendOutboundEmail"
      ],
      "Resource" : "arn:aws:connect:*:*:instance/*"
    },
    {
      "Sid" : "EventBridgeListRuleAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:ListRules"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EventBridgeManagedResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/ConnectCampaignsRule*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "events:ManagedBy" : "connect-campaigns.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EventBridgeListTargetsByRuleAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/ConnectCampaignsRule*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowWisdomForConnectCampaignsEnabledTaggedResources",
      "Effect" : "Allow",
      "Action" : [
        "wisdom:GetMessageTemplate",
        "wisdom:RenderMessageTemplate"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonConnectCampaignsEnabled" : "True"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonConnectReadOnlyAccess

説明: 内の Amazon Connect インスタンスを表示するアクセス許可を付与します AWS アカウント。

`AmazonConnectReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonConnectReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 10 月 17 日 21:00 UTC
- 編集日時: 2024 年 6 月 19 日 15:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonConnectReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonConnectServiceLinkedRolePolicy

説明: Amazon Connect がユーザーに代わって AWS リソースを作成および管理できるようにします。

`AmazonConnectServiceLinkedRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 9 月 7 日 00:21 UTC
- 編集日時: 2025 年 11 月 18 日 20:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonConnectServiceLinkedRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v31 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

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

```
      "Sid" : "AllowListLexBotAccess",
      "Effect" : "Allow",
      "Action" : [
        "lex:ListBots",
        "lex:ListBotAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCustomerProfilesForConnectDomain",
      "Effect" : "Allow",
      "Action" : [
        "profile:SearchProfiles",
        "profile:CreateProfile",
        "profile:UpdateProfile",
        "profile:AddProfileKey",
        "profile:ListProfileObjectTypes",
        "profile:ListCalculatedAttributeDefinitions",
        "profile:ListCalculatedAttributesForProfile",
        "profile:GetDomain",
        "profile:ListIntegrations",
        "profile:GetIntegration",
        "profile:PutIntegration",
        "profile:DeleteIntegration",
        "profile:ListEventTriggers",
        "profile:ListSegmentDefinitions",
        "profile:ListProfileAttributeValues",
        "profile:CreateSegmentEstimate",
        "profile:GetSegmentEstimate",
        "profile:BatchGetProfile",
        "profile:BatchGetCalculatedAttributeForProfile",
        "profile:GetSegmentMembership",
        "profile:ListDomainLayouts",
        "profile:CreateUploadJob",
        "profile:ListUploadJobs",
        "profile:DetectProfileObjectType",
        "profile:GetSimilarProfiles",
        "profile:GetUploadJob",
        "profile:GetUploadJobPath",
        "profile:StartUploadJob",
        "profile:StopUploadJob",
        "profile:GetProfileRecommendations",
        "profile:GetProfileInsights",
        "profile:ListRecommenders"
```

```
      ],
      "Resource" : "arn:aws:profile:*:*:domains/amazon-connect-*"
    },
    {
      "Sid" : "AllowCustomerProfilesEventTriggerForConnectDomain",
      "Effect" : "Allow",
      "Action" : [
        "profile:CreateEventTrigger",
        "profile:GetEventTrigger",
        "profile:UpdateEventTrigger",
        "profile:DeleteEventTrigger"
      ],
      "Resource" : [
        "arn:aws:profile:*:*:domains/amazon-connect-*/event-triggers/*"
      ]
    },
    {
      "Sid" : "AllowCustomerProfilesDomainLayoutsForConnectDomain",
      "Effect" : "Allow",
      "Action" : [
        "profile:CreateDomainLayout",
        "profile:UpdateDomainLayout",
        "profile:DeleteDomainLayout",
        "profile:GetDomainLayout"
      ],
      "Resource" : [
        "arn:aws:profile:*:*:domains/amazon-connect-*/layouts/*"
      ]
    },
    {
      "Sid" : "AllowCustomerProfilesSegmentationImportForConnectDomain",
      "Effect" : "Allow",
      "Action" : [
        "profile:GetUploadJob",
        "profile:GetUploadJobPath",
        "profile:StartUploadJob",
        "profile:StopUploadJob"
      ],
      "Resource" : [
        "arn:aws:profile:*:*:domains/amazon-connect-*/upload-jobs/*"
      ]
    },
    {
      "Sid" : "AllowReadPermissionForCustomerProfileObjects",
```

```
      "Effect" : "Allow",
      "Action" : [
        "profile:ListProfileObjects",
        "profile:GetProfileObjectType",
        "profile:ListObjectTypeAttributes",
        "profile:ListObjectTypeAttributeValues"
      ],
      "Resource" : [
        "arn:aws:profile:*:*:domains/amazon-connect-*/object-types/*"
      ]
    },
    {
      "Sid" : "AllowReadPermissionForCustomerProfilePredictiveInsights",
      "Effect" : "Allow",
      "Action" : [
        "profile:GetRecommender",
        "profile:CreateRecommender",
        "profile:UpdateRecommender",
        "profile:DeleteRecommender",
        "profile:StopRecommender",
        "profile:StartRecommender"
      ],
      "Resource" : [
        "arn:aws:profile:*:*:domains/amazon-connect-*/recommenders/*"
      ]
    },
    {
      "Sid" : "AllowReadPermissionForCustomerProfilesPersonalizeForRecommenderRecipes",
      "Effect" : "Allow",
      "Action" : [
        "profile:ListRecommenderRecipes"
      ],
      "Resource" : [
        "arn:aws:profile:*:*:*"
      ]
    },
    {
      "Sid" : "AllowListIntegrationForCustomerProfile",
      "Effect" : "Allow",
      "Action" : [
        "profile:ListAccountIntegrations"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "AllowReadForCustomerProfileObjectTemplates",
      "Effect" : "Allow",
      "Action" : [
        "profile:ListProfileObjectTypeTemplates",
        "profile:GetProfileObjectTypeTemplate"
      ],
      "Resource" : "arn:aws:profile:*:*:/templates*"
    },
    {
      "Sid" : "AllowAppIntegrationsForConnectEnabledTaggedResources",
      "Effect" : "Allow",
      "Action" : [
        "app-integrations:GetDataIntegration",
        "app-integrations:ListDataIntegrationAssociations",
        "app-integrations:CreateDataIntegrationSchedule",
        "app-integrations:StartDataIntegrationExecution",
        "app-integrations:ListDataIntegrationExecutions",
        "app-integrations:GetDataIntegrationExecution",
        "app-integrations:ListDataIntegrationSchedules",
        "app-integrations:UpdateDataIntegrationSchedule",
        "app-integrations:GetDataIntegrationSchedule"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonConnectEnabled" : "True"
        }
      }
    },
    {
      "Sid" : "AllowWisdomForConnectEnabledTaggedResources",
      "Effect" : "Allow",
      "Action" : [
        "wisdom:CreateContent",
        "wisdom:DeleteContent",
        "wisdom:CreateKnowledgeBase",
        "wisdom:GetAssistant",
        "wisdom:GetKnowledgeBase",
        "wisdom:GetContent",
        "wisdom:GetRecommendations",
        "wisdom:GetSession",
        "wisdom:NotifyRecommendationsReceived",
        "wisdom:QueryAssistant",
```

```
        "wisdom:StartContentUpload",
        "wisdom:UpdateContent",
        "wisdom:UntagResource",
        "wisdom:TagResource",
        "wisdom:CreateSession",
        "wisdom:CreateQuickResponse",
        "wisdom:GetQuickResponse",
        "wisdom:SearchQuickResponses",
        "wisdom:StartImportJob",
        "wisdom:GetImportJob",
        "wisdom:ListImportJobs",
        "wisdom:ListQuickResponses",
        "wisdom:UpdateQuickResponse",
        "wisdom:DeleteQuickResponse",
        "wisdom:PutFeedback",
        "wisdom:ListContentAssociations",
        "wisdom:CreateMessageTemplate",
        "wisdom:UpdateMessageTemplate",
        "wisdom:UpdateMessageTemplateMetadata",
        "wisdom:GetMessageTemplate",
        "wisdom:DeleteMessageTemplate",
        "wisdom:ListMessageTemplates",
        "wisdom:SearchMessageTemplates",
        "wisdom:ActivateMessageTemplate",
        "wisdom:DeactivateMessageTemplate",
        "wisdom:CreateMessageTemplateVersion",
        "wisdom:ListMessageTemplateVersions",
        "wisdom:CreateMessageTemplateAttachment",
        "wisdom:DeleteMessageTemplateAttachment",
        "wisdom:RenderMessageTemplate",
        "wisdom:CreateAIAgent",
        "wisdom:CreateAIAgentVersion",
        "wisdom:DeleteAIAgent",
        "wisdom:DeleteAIAgentVersion",
        "wisdom:UpdateAIAgent",
        "wisdom:UpdateAssistantAIAgent",
        "wisdom:RemoveAssistantAIAgent",
        "wisdom:GetAIAgent",
        "wisdom:ListAIAgents",
        "wisdom:ListAIAgentVersions",
        "wisdom:CreateAIPrompt",
        "wisdom:CreateAIPromptVersion",
        "wisdom:DeleteAIPrompt",
        "wisdom:DeleteAIPromptVersion",
```

```
        "wisdom:UpdateAIPrompt",
        "wisdom:GetAIPrompt",
        "wisdom:ListAIPrompts",
        "wisdom:ListAIPromptVersions",
        "wisdom:CreateAIGuardrail",
        "wisdom:CreateAIGuardrailVersion",
        "wisdom:DeleteAIGuardrail",
        "wisdom:DeleteAIGuardrailVersion",
        "wisdom:UpdateAIGuardrail",
        "wisdom:GetAIGuardrail",
        "wisdom:ListAIGuardrails",
        "wisdom:ListAIGuardrailVersions",
        "wisdom:CreateAssistant",
        "wisdom:ListTagsForResource",
        "wisdom:SendMessage",
        "wisdom:GetNextMessage",
        "wisdom:ListMessages",
        "wisdom:Retrieve",
        "wisdom:ListAssistantAssociations"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonConnectEnabled" : "True"
        }
      }
    },
    {
      "Sid" : "AllowListOperationForWisdom",
      "Effect" : "Allow",
      "Action" : [
        "wisdom:ListAssistants",
        "wisdom:ListKnowledgeBases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCustomerProfilesCalculatedAttributesForConnectDomain",
      "Effect" : "Allow",
      "Action" : [
        "profile:GetCalculatedAttributeForProfile",
        "profile:CreateCalculatedAttributeDefinition",
        "profile:DeleteCalculatedAttributeDefinition",
        "profile:GetCalculatedAttributeDefinition",
```

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

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

```
      ],
      "Resource" : "arn:aws:chime:*:*:vc/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SESPermissionsForManagingReceiptRules",
      "Effect" : "Allow",
      "Action" : [
        "ses:DescribeReceiptRule",
        "ses:UpdateReceiptRule"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SESPermissionForManagingConnectProvidedSESIdentity",
      "Effect" : "Allow",
      "Action" : [
        "ses:DeleteEmailIdentity"
      ],
      "Resource" : "arn:aws:ses:*:*:identity/*.email.connect.aws*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SESConfigurationSetPermissionsForSendingEmail",
      "Effect" : "Allow",
      "Action" : [
        "ses:SendRawEmail"
      ],
      "Resource" : "arn:aws:ses:*:*:configuration-set/configuration-set-for-connect-DO-
NOT-DELETE",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "PassRoleToSESForReceiptRuleManagement",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonConnectEmailSESAccessRole"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ses.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowSocialMessagingOperations",
      "Effect" : "Allow",
      "Action" : [
        "social-messaging:SendWhatsAppMessage",
        "social-messaging:PostWhatsAppMessageMedia",
        "social-messaging:GetWhatsAppMessageMedia",
        "social-messaging:GetLinkedWhatsAppBusinessAccountPhoneNumber"
      ],
      "Resource" : "arn:aws:social-messaging:*:*:phone-number-id/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonConnectEnabled" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowRetrievalOfWabas",
      "Effect" : "Allow",
      "Action" : [
        "social-messaging:ListLinkedWhatsAppBusinessAccounts"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowRetrievalOfWhatsAppTemplates",
      "Effect" : "Allow",
      "Action" : [
        "social-messaging:GetWhatsAppMessageTemplate",
        "social-messaging:ListWhatsAppMessageTemplates"
      ],
      "Resource" : "arn:aws:social-messaging:*:*:waba/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonConnectEnabled" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowMobileTargetingOperationsForConnect",
      "Effect" : "Allow",
      "Action" : "mobiletargeting:SendMessages",
      "Resource" : "arn:aws:mobiletargeting:*:*:apps/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowPollyActions",
      "Effect" : "Allow",
      "Action" : [
        "polly:ListLexicons",
        "polly:DescribeVoices",
        "polly:SynthesizeSpeech"
      ],
      "Resource" : [
        "*"
      ]
    }
```

```
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonConnectSynchronizationServiceRolePolicy

説明: Amazon Connect がユーザーに代わってリージョン間で AWS リソースを同期できるようにします。

`AmazonConnectSynchronizationServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 10 月 27 日 22:38 UTC
- 編集日時: 2025 年 11 月 21 日 20:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonConnectSynchronizationServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowConnectActions",
      "Effect" : "Allow",
      "Action" : [
        "connect:Create*",
        "connect:BatchCreate*",
        "connect:Update*",
        "connect:BatchUpdate*",
        "connect:Delete*",
        "connect:BatchDelete*",
        "connect:Describe*",
        "connect:BatchDescribe*",
        "connect:List*",
        "connect:Search*",
        "connect:Associate*",
        "connect:Disassociate*",
        "connect:Get*",
        "connect:BatchGet*",
        "connect:Import*",
        "connect:TagResource",
        "connect:UntagResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DisallowedConnectActions",
      "Effect" : "Deny",
      "Action" : [
        "connect:Start*",
        "connect:Stop*",
        "connect:Resume*",
        "connect:Suspend*",
        "connect:*Contact",
        "connect:SearchContacts",
        "connect:*ContactAttributes*",
        "connect:*RealtimeContact*",
        "connect:*AnalyticsData*",
        "connect:*MetricData*",
```

```
        "connect:*UserData*",
        "connect:*ContactEvaluation",
        "connect:*AttachedFile*",
        "connect:UpdateContactSchedule",
        "connect:UpdateContactRoutingData",
        "connect:ListContactReferences",
        "connect:CreateParticipant",
        "connect:CreatePersistentContactAssociation",
        "connect:CreateInstance",
        "connect:DeleteInstance",
        "connect:ListInstances",
        "connect:ReplicateInstance",
        "connect:GetFederationToken",
        "connect:ClaimPhoneNumber",
        "connect:ImportPhoneNumber",
        "connect:ReleasePhoneNumber",
        "connect:SearchAvailablePhoneNumbers",
        "connect:CreateTrafficDistributionGroup",
        "connect:DeleteTrafficDistributionGroup",
        "connect:GetTrafficDistribution",
        "connect:UpdateTrafficDistribution"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowPutMetricsForConnectNamespace",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Connect"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonConnectVoiceIDFullAccess

説明: Amazon Connect Voice ID へのフルアクセスを提供します

`AmazonConnectVoiceIDFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonConnectVoiceIDFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 9 月 26 日 19:04 UTC
- 編集日時: 2021 年 9 月 26 日 19:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonConnectVoiceIDFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonDataZoneBedrockModelConsumptionPolicy

説明: 特定の Amazon DataZone ドメイン用に作成された Amazon Bedrock アプリケーション推論プロファイルの呼び出しなど、Amazon Bedrock モデルを使用するアクセス許可を提供します。

`AmazonDataZoneBedrockModelConsumptionPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonDataZoneBedrockModelConsumptionPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2024 年 11 月 12 日 22:15 UTC
- 編集日時: 2025 年 5 月 28 日 18:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneBedrockModelConsumptionPolicy`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "InvokeDomainInferenceProfiles",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : "arn:aws:bedrock:*:*:application-inference-profile/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneDomain" : "${datazone:domainId}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "true"
        }
      }
    },
    {
      "Sid" : "ListFoundationModels",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:ListFoundationModels"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BedrockCreateSessionWithTagsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateSession",
        "bedrock:TagResource"
      ],
      "Resource" : "arn:aws:bedrock:*:*:session/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:RequestTag/AmazonDataZoneUser" : "${datazone:userId}",
```

```
          "aws:ResourceTag/AmazonDataZoneUser" : "${datazone:userId}",
          "aws:RequestTag/AmazonDataZoneDomain" : "${datazone:domainId}",
          "aws:ResourceTag/AmazonDataZoneDomain" : "${datazone:domainId}"
        },
        "StringNotEquals" : {
          "aws:RequestTag/AmazonDataZoneUser" : "",
          "aws:ResourceTag/AmazonDataZoneUser" : "",
          "aws:RequestTag/AmazonDataZoneDomain" : "",
          "aws:ResourceTag/AmazonDataZoneDomain" : ""
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "AmazonDataZone*"
        },
        "Null" : {
          "aws:RequestTag/AmazonDataZoneProject" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "true"
        }
      }
    },
    {
      "Sid" : "BedrockSessionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetSession",
        "bedrock:UpdateSession",
        "bedrock:DeleteSession",
        "bedrock:EndSession",
        "bedrock:CreateInvocation",
        "bedrock:ListInvocations",
        "bedrock:PutInvocationStep",
        "bedrock:GetInvocationStep",
        "bedrock:ListInvocationSteps",
        "bedrock:ListTagsForResource"
      ],
      "Resource" : "arn:aws:bedrock:*:*:session/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneUser" : "${datazone:userId}",
          "aws:ResourceTag/AmazonDataZoneDomain" : "${datazone:domainId}"
        },
        "StringNotEquals" : {
          "aws:ResourceTag/AmazonDataZoneUser" : "",
          "aws:ResourceTag/AmazonDataZoneDomain" : ""
```

```
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "true"
        }
      }
    },
    {
      "Sid" : "BedrockListSessionsPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:ListSessions",
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonDataZoneBedrockModelManagementPolicy

説明: アプリケーション推論プロファイルの作成、タグ付け、削除など、Amazon Bedrock モデルアクセスを管理するアクセス許可を提供します。

AmazonDataZoneBedrockModelManagementPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDataZoneBedrockModelManagementPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2024 年 11 月 12 日 22:14 UTC
- 編集日時: 2024 年 11 月 12 日 22:14 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ManageApplicationInferenceProfile",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateInferenceProfile",
        "bedrock:TagResource"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:application-inference-profile/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneProject"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:RequestTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
```

```
      "Sid" : "DeleteApplicationInferenceProfile",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:DeleteInferenceProfile"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:application-inference-profile/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "CreateApplicationInferenceProfileUsingFoundationModels",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateInferenceProfile"
      ],
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*"
      ]
    },
    {
      "Sid" : "CreateApplicationInferenceProfileUsingBedrockModels",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateInferenceProfile"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:inference-profile/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
```

```
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonDataZoneDomainExecutionRolePolicy

説明: Amazon DataZone の DomainExecutionRole サービスロールのデフォルトポリシー。このロールは、Amazon DataZone ドメイン内のデータをカタログ化、検出、管理、共有、分析するために Amazon DataZone で使用されます。

`AmazonDataZoneDomainExecutionRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonDataZoneDomainExecutionRolePolicy` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 9 月 27 日 21:55 UTC
- 編集日時: 2024 年 12 月 3 日 14:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneDomainExecutionRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v10 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DomainExecutionRoleStatement",
      "Effect" : "Allow",
      "Action" : [
        "datazone:AcceptPredictions",
        "datazone:AcceptSubscriptionRequest",
        "datazone:AddEntityOwner",
        "datazone:AddPolicyGrant",
        "datazone:CancelMetadataGenerationRun",
        "datazone:CancelSubscription",
        "datazone:CreateAsset",
        "datazone:CreateAssetFilter",
        "datazone:CreateAssetRevision",
        "datazone:CreateAssetType",
        "datazone:CreateDataProduct",
        "datazone:CreateDataProductRevision",
        "datazone:CreateDataSource",
        "datazone:CreateDomainUnit",
        "datazone:CreateEnvironment",
        "datazone:CreateEnvironmentBlueprint",
        "datazone:CreateEnvironmentProfile",
        "datazone:CreateFormType",
        "datazone:CreateGlossary",
        "datazone:CreateGlossaryTerm",
        "datazone:CreateListingChangeSet",
        "datazone:CreateProject",
        "datazone:CreateProjectMembership",
        "datazone:CreateRule",
        "datazone:CreateSubscriptionGrant",
        "datazone:CreateSubscriptionRequest",
        "datazone:DeleteAsset",
        "datazone:DeleteAssetFilter",
        "datazone:DeleteAssetType",
        "datazone:DeleteDataProduct",
        "datazone:DeleteDataSource",
        "datazone:DeleteDomainUnit",
        "datazone:DeleteEnvironment",
        "datazone:DeleteEnvironmentBlueprint",
```

```
        "datazone:DeleteEnvironmentProfile",
        "datazone:DeleteFormType",
        "datazone:DeleteGlossary",
        "datazone:DeleteGlossaryTerm",
        "datazone:DeleteListing",
        "datazone:DeleteProject",
        "datazone:DeleteProjectMembership",
        "datazone:DeleteRule",
        "datazone:DeleteSubscriptionGrant",
        "datazone:DeleteSubscriptionRequest",
        "datazone:DeleteSubscriptionTarget",
        "datazone:DeleteTimeSeriesDataPoints",
        "datazone:GetAsset",
        "datazone:GetAssetFilter",
        "datazone:GetAssetType",
        "datazone:GetDataProduct",
        "datazone:GetDataSource",
        "datazone:GetDataSourceRun",
        "datazone:GetDomain",
        "datazone:GetDomainUnit",
        "datazone:GetEnvironment",
        "datazone:GetEnvironmentAction",
        "datazone:GetEnvironmentActionLink",
        "datazone:GetEnvironmentBlueprint",
        "datazone:GetEnvironmentBlueprintConfiguration",
        "datazone:GetEnvironmentCredentials",
        "datazone:GetEnvironmentProfile",
        "datazone:GetFormType",
        "datazone:GetGlossary",
        "datazone:GetGlossaryTerm",
        "datazone:GetGroupProfile",
        "datazone:GetLineageNode",
        "datazone:GetListing",
        "datazone:GetMetadataGenerationRun",
        "datazone:GetProject",
        "datazone:GetRule",
        "datazone:GetSubscription",
        "datazone:GetSubscriptionEligibility",
        "datazone:GetSubscriptionGrant",
        "datazone:GetSubscriptionRequestDetails",
        "datazone:GetSubscriptionTarget",
        "datazone:GetTimeSeriesDataPoint",
        "datazone:GetUserProfile",
        "datazone:ListAccountEnvironments",
```

```
        "datazone:ListAssetFilters",
        "datazone:ListAssetRevisions",
        "datazone:ListDataProductRevisions",
        "datazone:ListDataSourceRunActivities",
        "datazone:ListDataSourceRuns",
        "datazone:ListDataSources",
        "datazone:ListDomainUnitsForParent",
        "datazone:ListEntityOwners",
        "datazone:ListEnvironmentActions",
        "datazone:ListEnvironmentBlueprintConfigurationSummaries",
        "datazone:ListEnvironmentBlueprintConfigurations",
        "datazone:ListEnvironmentBlueprints",
        "datazone:ListEnvironmentProfiles",
        "datazone:ListEnvironments",
        "datazone:ListGroupsForUser",
        "datazone:ListLineageNodeHistory",
        "datazone:ListMetadataGenerationRuns",
        "datazone:ListNotifications",
        "datazone:ListPolicyGrants",
        "datazone:ListProjectMemberships",
        "datazone:ListProjects",
        "datazone:ListRules",
        "datazone:ListSubscriptionGrants",
        "datazone:ListSubscriptionRequests",
        "datazone:ListSubscriptionTargets",
        "datazone:ListSubscriptions",
        "datazone:ListTimeSeriesDataPoints",
        "datazone:ListWarehouseMetadata",
        "datazone:RejectPredictions",
        "datazone:RejectSubscriptionRequest",
        "datazone:RemoveEntityOwner",
        "datazone:RemovePolicyGrant",
        "datazone:RevokeSubscription",
        "datazone:Search",
        "datazone:SearchGroupProfiles",
        "datazone:SearchListings",
        "datazone:SearchRules",
        "datazone:SearchTypes",
        "datazone:SearchUserProfiles",
        "datazone:StartDataSourceRun",
        "datazone:StartMetadataGenerationRun",
        "datazone:UpdateAssetFilter",
        "datazone:UpdateDataSource",
        "datazone:UpdateDomainUnit",
```

```
        "datazone:UpdateEnvironment",
        "datazone:UpdateEnvironmentBlueprint",
        "datazone:UpdateEnvironmentDeploymentStatus",
        "datazone:UpdateEnvironmentProfile",
        "datazone:UpdateGlossary",
        "datazone:UpdateGlossaryTerm",
        "datazone:UpdateProject",
        "datazone:UpdateRule",
        "datazone:UpdateSubscriptionGrantStatus",
        "datazone:UpdateSubscriptionRequest"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RAMResourceShareStatement",
      "Effect" : "Allow",
      "Action" : "ram:GetResourceShareAssociations",
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonDataZoneEnvironmentRolePermissionsBoundary

説明: Amazon DataZone はデータ分析アクションを実行する環境用の IAM ロールを作成しますが、それらのロールの作成時にこのポリシーを使用してアクセス許可の範囲を定義します。

`AmazonDataZoneEnvironmentRolePermissionsBoundary` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonDataZoneEnvironmentRolePermissionsBoundary` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 9 月 11 日 23:38 UTC
- 編集日時: 2023 年 11 月 17 日 23:29 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneEnvironmentRolePermissionsBoundary`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonDataZoneFullAccess

説明: 経由で Amazon DataZone へのフルアクセス AWS マネジメントコンソール と、それに必要な関連サービスへの制限付きアクセスを提供します。

`AmazonDataZoneFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonDataZoneFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 9 月 22 日 20:06 UTC
- 編集日時: 2025 年 7 月 23 日 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonDataZoneStatement",
      "Effect" : "Allow",
      "Action" : [
        "datazone:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ReadOnlyStatement",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "iam:ListRoles",
        "sso:DescribeRegisteredRegions",
        "s3:ListAllMyBuckets",
        "redshift:DescribeClusters",
        "redshift-serverless:ListWorkgroups",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "secretsmanager:ListSecrets",
        "iam:ListUsers",
        "glue:GetDatabases",
        "codeconnections:ListConnections",
        "codeconnections:ListTagsForResource",
        "codewhisperer:ListProfiles",
        "bedrock:ListInferenceProfiles",
        "bedrock:ListFoundationModels",
        "bedrock:ListTagsForResource",
        "aoss:ListSecurityPolicies"
```

```
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "BucketReadOnlyStatement",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "CreateBucketStatement",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::amazon-datazone*",
        "arn:aws:s3:::amazon-sagemaker*"
      ]
    },
    {
      "Sid" : "ConfigureBucketStatement",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketCORS",
        "s3:PutBucketPolicy",
        "s3:PutBucketVersioning"
      ],
      "Resource" : [
        "arn:aws:s3:::amazon-sagemaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RamCreateResourceStatement",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "ram:RequestedResourceType" : "datazone:Domain"
        }
      }
    },
    {
      "Sid" : "RamResourceStatement",
      "Effect" : "Allow",
      "Action" : [
        "ram:DeleteResourceShare",
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare",
        "ram:RejectResourceShareInvitation"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ram:ResourceShareName" : [
            "DataZone*"
          ]
        }
      }
    },
    {
      "Sid" : "RamResourceReadOnlyStatement",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShares",
        "ram:GetResourceShareInvitations",
        "ram:GetResourceShareAssociations",
        "ram:ListResourceSharePermissions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RamAssociateResourceSharePermissionStatement",
      "Effect" : "Allow",
      "Action" : "ram:AssociateResourceSharePermission",
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ram:PermissionArn" : [
            "arn:aws:ram::aws:permission/AWSRAMDefaultPermissionAmazonDataZoneDomain",
            "arn:aws:ram::aws:permission/
AWSRAMPermissionAmazonDataZoneDomainFullAccessWithPortalAccess",
            "arn:aws:ram::aws:permission/
AWSRAMPermissionsAmazonDatazoneDomainExtendedServiceAccess",
            "arn:aws:ram::aws:permission/
AWSRAMPermissionsAmazonDatazoneDomainExtendedServiceWithPortalAccess"
          ]
        }
      }
    },
    {
      "Sid" : "IAMPassRoleStatement",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/AmazonDataZone*",
        "arn:aws:iam::*:role/service-role/AmazonDataZone*",
        "arn:aws:iam::*:role/service-role/AmazonSageMaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:passedToService" : "datazone.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMGetPolicyStatement",
      "Effect" : "Allow",
      "Action" : "iam:GetPolicy",
      "Resource" : [
        "arn:aws:iam::*:policy/service-role/AmazonDataZoneRedshiftAccessPolicy*"
      ]
    },
    {
      "Sid" : "DataZoneTagOnCreateDomainProjectTags",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource"
      ],
```

```
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneDomain",
            "AmazonDataZoneProject"
          ]
        },
        "StringLike" : {
          "aws:RequestTag/AmazonDataZoneDomain" : "dzd*",
          "aws:ResourceTag/AmazonDataZoneDomain" : "dzd*"
        }
      }
    },
    {
      "Sid" : "DataZoneTagOnCreate",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneDomain"
          ]
        },
        "StringLike" : {
          "aws:RequestTag/AmazonDataZoneDomain" : "dzd*",
          "aws:ResourceTag/AmazonDataZoneDomain" : "dzd*"
        }
      }
    },
    {
      "Sid" : "CreateSecretStatement",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AmazonDataZoneDomain" : "dzd*"
        }
```

```
      }
    },
    {
      "Sid" : "ConnectionStatement",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:GetConnection"
      ],
      "Resource" : [
        "arn:aws:codeconnections:*:*:connection/*"
      ]
    },
    {
      "Sid" : "TagCodeConnectionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:TagResource"
      ],
      "Resource" : [
        "arn:aws:codeconnections:*:*:connection/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "for-use-with-all-datazone-projects"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "UntagCodeConnectionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:UntagResource"
      ],
      "Resource" : [
        "arn:aws:codeconnections:*:*:connection/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "for-use-with-all-datazone-projects"
```

```
        }
      }
    },
    {
      "Sid" : "SSMParameterStatement",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:GetParametersByPath",
        "ssm:PutParameter",
        "ssm:DeleteParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/amazon/datazone/q*",
        "arn:aws:ssm:*:*:parameter/amazon/datazone/genAI*",
        "arn:aws:ssm:*:*:parameter/amazon/datazone/profiles*"
      ]
    },
    {
      "Sid" : "UseKMSKeyPermissionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/EnableKeyForAmazonDataZone" : "true"
        },
        "Null" : {
          "aws:ResourceTag/EnableKeyForAmazonDataZone" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "ssm.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SecurityPolicyStatement",
      "Effect" : "Allow",
      "Action" : [
        "aoss:GetSecurityPolicy",
```

```
        "aoss:CreateSecurityPolicy"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "aoss:collection" : "genai-studio-*"
        }
      }
    },
    {
      "Sid" : "GetFoundationModelStatement",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetFoundationModel",
        "bedrock:GetFoundationModelAvailability"
      ],
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*"
      ]
    },
    {
      "Sid" : "GetInferenceProfileStatement",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetInferenceProfile"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:inference-profile/*",
        "arn:aws:bedrock:*:*:application-inference-profile/*"
      ]
    },
    {
      "Sid" : "ApplicationInferenceProfileStatement",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateInferenceProfile"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:application-inference-profile/*"
      ],
      "Condition" : {
        "Null" : {
```

```
          "aws:RequestTag/AmazonDataZoneProject" : "true",
          "aws:RequestTag/AmazonDataZoneDomain" : "false"
        }
      }
    },
    {
      "Sid" : "TagApplicationInferenceProfileStatement",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:TagResource"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:application-inference-profile/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "true",
          "aws:RequestTag/AmazonDataZoneProject" : "true",
          "aws:ResourceTag/AmazonDataZoneDomain" : "false",
          "aws:RequestTag/AmazonDataZoneDomain" : "false"
        }
      }
    },
    {
      "Sid" : "DeleteApplicationInferenceProfileStatement",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:DeleteInferenceProfile"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:application-inference-profile/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "true",
          "aws:ResourceTag/AmazonDataZoneDomain" : "false"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonDataZoneFullUserAccess

説明: Amazon DataZone へのフルアクセスを提供しますが、ドメイン、ユーザー、または関連するアカウントの管理は許可しません。

`AmazonDataZoneFullUserAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonDataZoneFullUserAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 9 月 22 日 21:06 UTC
- 編集日時: 2024 年 11 月 19 日 21:38 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneFullUserAccess`

ポリシーのバージョン

ポリシーのバージョン: v9 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
  "Statement" : [
    {
      "Sid" : "AmazonDataZoneUserOperations",
      "Effect" : "Allow",
      "Action" : [
        "datazone:AcceptPredictions",
        "datazone:AcceptSubscriptionRequest",
        "datazone:AddEntityOwner",
        "datazone:AddPolicyGrant",
        "datazone:CancelMetadataGenerationRun",
        "datazone:CancelSubscription",
        "datazone:CreateAsset",
        "datazone:CreateAssetFilter",
        "datazone:CreateAssetRevision",
        "datazone:CreateAssetType",
        "datazone:CreateDataProduct",
        "datazone:CreateDataProductRevision",
        "datazone:CreateDataSource",
        "datazone:CreateDomainUnit",
        "datazone:CreateEnvironment",
        "datazone:CreateEnvironmentBlueprint",
        "datazone:CreateEnvironmentProfile",
        "datazone:CreateFormType",
        "datazone:CreateGlossary",
        "datazone:CreateGlossaryTerm",
        "datazone:CreateListingChangeSet",
        "datazone:CreateProject",
        "datazone:CreateProjectMembership",
        "datazone:CreateRule",
        "datazone:CreateSubscriptionGrant",
        "datazone:CreateSubscriptionRequest",
        "datazone:DeleteAsset",
        "datazone:DeleteAssetFilter",
        "datazone:DeleteAssetType",
        "datazone:DeleteDataProduct",
        "datazone:DeleteDataSource",
        "datazone:DeleteDomainUnit",
        "datazone:DeleteEnvironment",
        "datazone:DeleteEnvironmentBlueprint",
        "datazone:DeleteEnvironmentProfile",
        "datazone:DeleteFormType",
        "datazone:DeleteGlossary",
        "datazone:DeleteGlossaryTerm",
        "datazone:DeleteListing",
```

```
            "datazone:DeleteProject",
            "datazone:DeleteProjectMembership",
            "datazone:DeleteRule",
            "datazone:DeleteSubscriptionGrant",
            "datazone:DeleteSubscriptionRequest",
            "datazone:DeleteSubscriptionTarget",
            "datazone:DeleteTimeSeriesDataPoints",
            "datazone:GetAsset",
            "datazone:GetAssetFilter",
            "datazone:GetAssetType",
            "datazone:GetDataProduct",
            "datazone:GetDataSource",
            "datazone:GetDataSourceRun",
            "datazone:GetDomain",
            "datazone:GetDomainUnit",
            "datazone:GetEnvironment",
            "datazone:GetEnvironmentActionLink",
            "datazone:GetEnvironmentBlueprint",
            "datazone:GetEnvironmentCredentials",
            "datazone:GetEnvironmentProfile",
            "datazone:GetFormType",
            "datazone:GetGlossary",
            "datazone:GetGlossaryTerm",
            "datazone:GetGroupProfile",
            "datazone:GetIamPortalLoginUrl",
            "datazone:GetLineageNode",
            "datazone:GetListing",
            "datazone:GetMetadataGenerationRun",
            "datazone:GetProject",
            "datazone:GetRule",
            "datazone:GetSubscription",
            "datazone:GetSubscriptionEligibility",
            "datazone:GetSubscriptionGrant",
            "datazone:GetSubscriptionRequestDetails",
            "datazone:GetSubscriptionTarget",
            "datazone:GetTimeSeriesDataPoint",
            "datazone:GetUserProfile",
            "datazone:ListAccountEnvironments",
            "datazone:ListAssetFilters",
            "datazone:ListAssetRevisions",
            "datazone:ListDataProductRevisions",
            "datazone:ListDataSourceRunActivities",
            "datazone:ListDataSourceRuns",
            "datazone:ListDataSources",
```

```
        "datazone:ListDomainUnitsForParent",
        "datazone:ListEntityOwners",
        "datazone:ListEnvironmentBlueprintConfigurations",
        "datazone:ListEnvironmentBlueprints",
        "datazone:ListEnvironmentProfiles",
        "datazone:ListEnvironments",
        "datazone:ListGroupsForUser",
        "datazone:ListLineageNodeHistory",
        "datazone:ListMetadataGenerationRuns",
        "datazone:ListNotifications",
        "datazone:ListPolicyGrants",
        "datazone:ListProjectMemberships",
        "datazone:ListProjects",
        "datazone:ListRules",
        "datazone:ListSubscriptionGrants",
        "datazone:ListSubscriptionRequests",
        "datazone:ListSubscriptionTargets",
        "datazone:ListSubscriptions",
        "datazone:ListTimeSeriesDataPoints",
        "datazone:ListWarehouseMetadata",
        "datazone:PostTimeSeriesDataPoints",
        "datazone:RejectPredictions",
        "datazone:RejectSubscriptionRequest",
        "datazone:RemoveEntityOwner",
        "datazone:RemovePolicyGrant",
        "datazone:RevokeSubscription",
        "datazone:Search",
        "datazone:SearchGroupProfiles",
        "datazone:SearchListings",
        "datazone:SearchRules",
        "datazone:SearchTypes",
        "datazone:SearchUserProfiles",
        "datazone:StartDataSourceRun",
        "datazone:StartMetadataGenerationRun",
        "datazone:UpdateAssetFilter",
        "datazone:UpdateDataSource",
        "datazone:UpdateDomainUnit",
        "datazone:UpdateEnvironment",
        "datazone:UpdateEnvironmentBlueprint",
        "datazone:UpdateEnvironmentDeploymentStatus",
        "datazone:UpdateEnvironmentProfile",
        "datazone:UpdateGlossary",
        "datazone:UpdateGlossaryTerm",
        "datazone:UpdateProject",
```

```
        "datazone:UpdateRule",
        "datazone:UpdateSubscriptionGrantStatus",
        "datazone:UpdateSubscriptionRequest"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RAMResourceShareOperations",
      "Effect" : "Allow",
      "Action" : "ram:GetResourceShareAssociations",
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonDataZoneGlueManageAccessRolePolicy

説明: このポリシーは、Amazon DataZone がデータを公開し、データ権限にアクセスすることを許可します。

AmazonDataZoneGlueManageAccessRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDataZoneGlueManageAccessRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 9 月 22 日 20:21 UTC
- 編集日時: 2025 年 6 月 19 日 19:37 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v10 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GlueTagDatabase",
      "Effect" : "Allow",
      "Action" : [
        "glue:TagResource",
        "glue:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ForAnyValue:StringLikeIfExists" : {
          "aws:TagKeys" : "DataZoneDiscoverable_*"
        }
      }
    },
    {
      "Sid" : "GlueDataQuality",
      "Effect" : "Allow",
      "Action" : [
        "glue:ListDataQualityResults",
        "glue:GetDataQualityResult"
      ],
      "Resource" : "arn:aws:glue:*:*:dataQualityRuleset/*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueCrawler",
      "Effect" : "Allow",
      "Action" : "glue:ListCrawls",
      "Resource" : "arn:aws:glue:*:*:crawler/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueConnection",
      "Effect" : "Allow",
      "Action" : "glue:GetConnection",
      "Resource" : [
        "arn:aws:glue:*:*:connection/*",
        "arn:aws:glue:*:*:catalog"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueTableDatabaseCatalog",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateTable",
        "glue:DeleteTable",
        "glue:GetDatabases",
        "glue:GetTables",
        "glue:SearchTables",
        "glue:CreateCatalog",
        "glue:CreateDatabase",
        "glue:DeleteCatalog",
        "glue:DeleteDatabase"
      ],
```

```
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:userDefinedFunction/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueGetTags",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetTags",
        "glue:GetCatalog"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:database/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "LakeformationResourceSharing",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:BatchGrantPermissions",
        "lakeformation:BatchRevokePermissions",
        "lakeformation:CreateDataCellsFilter",
        "lakeformation:CreateLakeFormationOptIn",
        "lakeformation:DeleteDataCellsFilter",
        "lakeformation:DeleteLakeFormationOptIn",
        "lakeformation:GrantPermissions",
        "lakeformation:GetDataCellsFilter",
        "lakeformation:GetResourceLFTags",
```

```
        "lakeformation:ListDataCellsFilter",
        "lakeformation:ListLakeFormationOptIns",
        "lakeformation:ListPermissions",
        "lakeformation:RegisterResource",
        "lakeformation:RevokePermissions",
        "lakeformation:UpdateDataCellsFilter",
        "glue:GetDatabase",
        "glue:GetTable",
        "organizations:DescribeOrganization",
        "ram:GetResourceShareInvitations",
        "ram:ListResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LakeformationResourceFederatedSharing",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "lakeformation:GlueARN" : "true"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "glue.amazonaws.com",
            "lakeformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CrossAccountRAMResourceSharing",
      "Effect" : "Allow",
      "Action" : [
        "glue:DeleteResourcePolicy",
        "glue:PutResourcePolicy"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:database/*",
```

```
        "arn:aws:glue:*:*:table/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "ram.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CrossAccountLakeFormationResourceSharing",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "ram:RequestedResourceType" : [
            "glue:Table",
            "glue:Database",
            "glue:Catalog"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "lakeformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CrossAccountRAMResourceShareInvitation",
      "Effect" : "Allow",
      "Action" : [
        "ram:AcceptResourceShareInvitation"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share-invitation/*"
    },
    {
      "Sid" : "CrossAccountRAMResourceSharingViaLakeFormation",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ram:AssociateResourceShare",
        "ram:DeleteResourceShare",
        "ram:DisassociateResourceShare",
        "ram:ListResourceSharePermissions",
        "ram:UpdateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ram:ResourceShareName" : [
            "LakeFormation*"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "lakeformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "GetResourceSharesViaLakeFormation",
      "Effect" : "Allow",
      "Action" : "ram:GetResourceShares",
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "lakeformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CrossAccountRAMResourceSharingViaLakeFormationHybrid",
      "Effect" : "Allow",
      "Action" : "ram:AssociateResourceSharePermission",
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ram:PermissionArn" : "arn:aws:ram::aws:permission/AWSRAMLFEnabled*"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
```

```
            "lakeformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "KMSDecrypt",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/datazone:projectId" : "proj-all"
        }
      }
    },
    {
      "Sid" : "GetRoleForDataZone",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AmazonDataZone*",
        "arn:aws:iam::*:role/service-role/AmazonDataZone*",
        "arn:aws:iam::*:role/AmazonSageMakerManageAccess*",
        "arn:aws:iam::*:role/service-role/AmazonSageMakerManageAccess*"
      ]
    },
    {
      "Sid" : "PassRoleForDataLocationRegistration",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AmazonDataZone*",
        "arn:aws:iam::*:role/service-role/AmazonDataZone*",
        "arn:aws:iam::*:role/AmazonSageMakerManageAccess*",
        "arn:aws:iam::*:role/service-role/AmazonSageMakerManageAccess*",
        "arn:aws:iam::*:role/datazone_usr_role*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lakeformation.amazonaws.com",
            "glue.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreateCatalogEC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateCatalogS3",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:PutBucketPolicy",
        "s3:PutEncryptionConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketVersioning",
        "s3:PutBucketTagging"
      ],
      "Resource" : "arn:aws:s3:::redshift-staging-bucket*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonDataZonePortalFullAccessPolicy

説明: Amazon DataZone API へのフルアクセスを提供します

AmazonDataZonePortalFullAccessPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDataZonePortalFullAccessPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 3 月 26 日 18:24 UTC
- 編集日時: 2023 年 3 月 26 日 18:24 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDataZonePortalFullAccessPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "datazonecontrol:*",
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonDataZonePreviewConsoleFullAccess

説明: AWS マネジメントコンソール経由で Amazon DataZone のプレビューリリースへのフルアクセスを提供します。関連サービスへの限定アクセスも提供します。

AmazonDataZonePreviewConsoleFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDataZonePreviewConsoleFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 3 月 28 日 15:16 UTC
- 編集日時: 2023 年 7 月 13 日 18:01 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDataZonePreviewConsoleFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonDataZoneProjectDeploymentPermissionsBoundary

説明: Amazon DataZone がデータ分析プロジェクトのデプロイに使用する IAM ロールを作成します。DataZone はこれらのロールを作成する際にこのポリシーを使用してアクセス許可の境界を定義します。

`AmazonDataZoneProjectDeploymentPermissionsBoundary` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonDataZoneProjectDeploymentPermissionsBoundary` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 3 月 21 日 02:54 UTC
- 編集日時: 2023 年 4 月 4 日 02:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneProjectDeploymentPermissionsBoundary`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonDataZoneProjectRolePermissionsBoundary

説明: Amazon DataZone はデータ分析アクションを実行するプロジェクト用の IAM ロールを作成しますが、それらのロール作成時にこのポリシーを使用してアクセス許可の範囲を定義します。

AmazonDataZoneProjectRolePermissionsBoundary は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDataZoneProjectRolePermissionsBoundary をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 3 月 21 日 02:51 UTC
- 編集日時: 2023 年 3 月 21 日 02:51 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDataZoneProjectRolePermissionsBoundary

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonDataZoneRedshiftGlueProvisioningPolicy

説明: Amazon DataZone は、データのカタログ化、検出、管理、共有、分析を可能にするデータ管理サービスです。Amazon DataZone では、アカウントやサポートされているリージョン間でデータを共有し、アクセスできます。Amazon DataZone は、Amazon Redshift、Amazon Athena、 AWS Glue、 AWS Lake Formation などの AWS サービス間のエクスペリエンスを簡素化します。

`AmazonDataZoneRedshiftGlueProvisioningPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonDataZoneRedshiftGlueProvisioningPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 9 月 22 日 20:19 UTC
- 編集日時: 2024 年 10 月 23 日 18:29 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneRedshiftGlueProvisioningPolicy`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
        "iam:DetachRolePolicy",
        "iam:DeleteRolePolicy",
        "iam:AttachRolePolicy",
        "iam:PutRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/datazone*",
      "Condition" : {
        "StringEquals" : {
          "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/
AmazonDataZoneEnvironmentRolePermissionsBoundary",
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "IamPassRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com",
            "lakeformation.amazonaws.com"
          ],
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZonePermissionsToManageCreatedEnvironmentRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole",
        "iam:GetRole"
      ],
```

```
      "Resource" : "arn:aws:iam::*:role/datazone*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneCFStackCreationForEnvironments",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:TagResource"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*"
      ],
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : "AmazonDataZoneEnvironment"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneCFStackManagementForEnvironments",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*"
      ]
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentParameterValidation",
      "Effect" : "Allow",
      "Action" : [
```

```
        "lakeformation:GetDataLakeSettings",
        "lakeformation:PutDataLakeSettings",
        "lakeformation:RevokePermissions",
        "lakeformation:ListPermissions",
        "glue:CreateDatabase",
        "glue:GetDatabase",
        "athena:GetWorkGroup",
        "logs:DescribeLogGroups",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift:DescribeClusters",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentLakeFormationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:RegisterResource",
        "lakeformation:DeregisterResource",
        "lakeformation:GrantPermissions",
        "lakeformation:ListResources"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentGlueDeletePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:DeleteDatabase"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentAthenaDeletePermissions",
      "Effect" : "Allow",
      "Action" : [
        "athena:DeleteWorkGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentAthenaResourceCreation",
      "Effect" : "Allow",
      "Action" : [
        "athena:CreateWorkGroup",
        "athena:TagResource",
        "iam:TagRole",
        "iam:TagPolicy",
        "logs:TagLogGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : "AmazonDataZoneEnvironment"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        },
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
```

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

```
        "iam:ListPolicyVersions",
        "iam:DeletePolicyVersion"
      ],
      "Resource" : [
        "arn:aws:iam::*:policy/datazone*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentS3ValidationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentKMSDecryptPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "PermissionsToTagAmazonDataZoneEnvironmentGlueResources",
      "Effect" : "Allow",
      "Action" : [
        "glue:TagResource"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : "AmazonDataZoneEnvironment"
        },
        "Null" : {
          "aws:RequestTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "PermissionsToGetAmazonDataZoneEnvironmentBlueprintTemplates",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "RedshiftDataPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:ListSchemas",
        "redshift-data:ExecuteStatement"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:workgroup/*",
        "arn:aws:redshift:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "DescribeStatementPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:DescribeStatement"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "GetSecretValuePermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:ResourceTag/AmazonDataZoneDomain" : "dzd*"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonDataZoneRedshiftManageAccessRolePolicy

説明: このポリシーは、Amazon Redshift データをカタログに公開するためのアクセス許可を Amazon DataZone に付与します。また、Amazon Redshift または Amazon Redshift Serverless がカタログに公開したアセットへのアクセス権の付与や、アクセス権の取り消しを行うためのアクセス許可も Amazon DataZone に付与します。

`AmazonDataZoneRedshiftManageAccessRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonDataZoneRedshiftManageAccessRolePolicy` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 9 月 22 日 20:15 UTC
- 編集日時: 2025 年 3 月 7 日 00:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneRedshiftManageAccessRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "redshiftDataScopeDownPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:BatchExecuteStatement",
        "redshift-data:DescribeTable",
        "redshift-data:ExecuteStatement",
        "redshift-data:ListTables",
        "redshift-data:ListSchemas",
        "redshift-data:ListDatabases"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:workgroup/*",
        "arn:aws:redshift:*:*:cluster:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "listSecretsPermission",
      "Effect" : "Allow",
      "Action" : "secretsmanager:ListSecrets",
      "Resource" : "*"
    },
    {
      "Sid" : "getWorkgroupPermission",
      "Effect" : "Allow",
      "Action" : "redshift-serverless:GetWorkgroup",
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:workgroup/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "createAndDeleteWorkgroupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:CreateWorkgroup",
        "redshift-serverless:DeleteWorkgroup"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:workgroup/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "glue.amazonaws.com",
            "lakeformation.amazonaws.com"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "getNamespacePermission",
      "Effect" : "Allow",
      "Action" : "redshift-serverless:GetNamespace",
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "createAndDeleteNamespacePermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:CreateNamespace",
        "redshift-serverless:DeleteNamespace"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "glue.amazonaws.com",
            "lakeformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "redshiftDataPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:DescribeStatement",
        "redshift-data:GetStatementResult",
        "redshift:DescribeClusters"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "dataSharesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:AuthorizeDataShare",
        "redshift:DescribeDataShares"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:datashare:*/datazone*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "associateDataShareConsumerPermission",
      "Effect" : "Allow",
      "Action" : "redshift:AssociateDataShareConsumer",
      "Resource" : "arn:aws:redshift:*:*:datashare:*/datazone*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary

説明 : AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary ポリシーは、Amazon DataZone によってプロビジョニングされた SageMaker 環境で作成される実行ロールに付与されるアクセス許可のリストです。

`AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 4 月 23 日 23:01 UTC
- 編集日時: 2025 年 11 月 17 日 18:34 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowAllNonAdminSageMakerActions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:*",
        "sagemaker-geospatial:*"
      ],
      "NotResource" : [
        "arn:aws:sagemaker:*:*:domain/*",
        "arn:aws:sagemaker:*:*:user-profile/*",
        "arn:aws:sagemaker:*:*:app/*",
        "arn:aws:sagemaker:*:*:space/*",
        "arn:aws:sagemaker:*:*:flow-definition/*"
      ]
```

```
    },
    {
      "Sid" : "AllowSageMakerProfileManagement",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateUserProfile",
        "sagemaker:DescribeUserProfile",
        "sagemaker:UpdateUserProfile",
        "sagemaker:CreatePresignedDomainUrl"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:*/*"
    },
    {
      "Sid" : "AllowLakeFormation",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataAccess"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAddTagsForDomainResources",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:app/*",
        "arn:aws:sagemaker:*:*:space/*",
        "arn:aws:sagemaker:*:*:user-profile/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "sagemaker:TaggingAction" : [
            "CreateApp",
            "CreateSpace",
            "CreateUserProfile"
          ]
        }
      }
    },
    {
      "Sid" : "AllowStudioActions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "sagemaker:CreatePresignedDomainUrl",
        "sagemaker:DescribeApp",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeSpace",
        "sagemaker:DescribeUserProfile",
        "sagemaker:ListApps",
        "sagemaker:ListDomains",
        "sagemaker:ListSpaces",
        "sagemaker:ListUserProfiles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAppActionsForUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateApp",
        "sagemaker:DeleteApp"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:app/*/*/*/*",
      "Condition" : {
        "Null" : {
          "sagemaker:OwnerUserProfileArn" : "true"
        }
      }
    },
    {
      "Sid" : "AllowAppActionsForSharedSpaces",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateApp",
        "sagemaker:DeleteApp"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:app/${sagemaker:DomainId}/*/*/*",
      "Condition" : {
        "StringEquals" : {
          "sagemaker:SpaceSharingType" : [
            "Shared"
          ]
        }
      }
    },
    {
```

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

```
      "Condition" : {
        "ArnLike" : {
          "sagemaker:OwnerUserProfileArn" : "arn:aws:sagemaker:*:*:user-profile/
${sagemaker:DomainId}/${sagemaker:UserProfileName}"
        },
        "StringEquals" : {
          "sagemaker:SpaceSharingType" : [
            "Private"
          ]
        }
      }
    },
    {
      "Sid" : "AllowFlowDefinitionActions",
      "Effect" : "Allow",
      "Action" : "sagemaker:*",
      "Resource" : [
        "arn:aws:sagemaker:*:*:flow-definition/*"
      ],
      "Condition" : {
        "StringEqualsIfExists" : {
          "sagemaker:WorkteamType" : [
            "private-crowd",
            "vendor-crowd"
          ]
        }
      }
    },
    {
      "Sid" : "AllowAWSServiceActions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:*",
        "datazone:*",
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeleteScheduledAction",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:PutScheduledAction",
        "application-autoscaling:RegisterScalableTarget",
```

```
        "aws-marketplace:ViewSubscriptions",
        "cloudformation:GetTemplateSummary",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:PutMetricData",
        "codecommit:BatchGetRepositories",
        "codecommit:CreateRepository",
        "codecommit:GetRepository",
        "codecommit:List*",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeVpcs",
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:Describe*",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer",
        "ecr:StartImageScan",
        "elastic-inference:Connect",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets",
        "fsx:DescribeFileSystems",
        "groundtruthlabeling:*",
        "iam:GetRole",
        "iam:ListRoles",
        "kms:DescribeKey",
        "kms:ListAliases",
        "lambda:ListFunctions",
        "logs:CreateLogDelivery",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
```

```
        "logs:DeleteLogDelivery",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:GetLogDelivery",
        "logs:GetLogEvents",
        "logs:ListLogDeliveries",
        "logs:PutLogEvents",
        "logs:UpdateLogDelivery",
        "redshift-data:BatchExecuteStatement",
        "redshift-data:CancelStatement",
        "redshift-data:DescribeStatement",
        "redshift-data:DescribeTable",
        "redshift-data:ExecuteStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables",
        "redshift-serverless:GetCredentials",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "secretsmanager:ListSecrets",
        "servicecatalog:Describe*",
        "servicecatalog:List*",
        "servicecatalog:ScanProvisionedProducts",
        "servicecatalog:SearchProducts",
        "servicecatalog:SearchProvisionedProducts",
        "sns:ListTopics",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowRAMInvitation",
      "Effect" : "Allow",
      "Action" : "ram:AcceptResourceShareInvitation",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ram:ResourceShareName" : "dzd*"
        }
      }
    },
    {
```

```
      "Sid" : "AllowECRActions",
      "Effect" : "Allow",
      "Action" : [
        "ecr:SetRepositoryPolicy",
        "ecr:CompleteLayerUpload",
        "ecr:CreateRepository",
        "ecr:BatchDeleteImage",
        "ecr:UploadLayerPart",
        "ecr:DeleteRepositoryPolicy",
        "ecr:InitiateLayerUpload",
        "ecr:DeleteRepository",
        "ecr:PutImage",
        "ecr:TagResource",
        "ecr:UntagResource"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/sagemaker*",
        "arn:aws:ecr:*:*:repository/datazone*"
      ]
    },
    {
      "Sid" : "AllowCodeCommitActions",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:GitPull",
        "codecommit:GitPush"
      ],
      "Resource" : [
        "arn:aws:codecommit:*:*:*sagemaker*",
        "arn:aws:codecommit:*:*:*SageMaker*",
        "arn:aws:codecommit:*:*:*Sagemaker*"
      ]
    },
    {
      "Sid" : "AllowCodeBuildActions",
      "Action" : [
        "codebuild:BatchGetBuilds",
        "codebuild:StartBuild"
      ],
      "Resource" : [
        "arn:aws:codebuild:*:*:project/sagemaker*",
        "arn:aws:codebuild:*:*:build/*"
      ],
      "Effect" : "Allow"
```

```
    },
    {
      "Sid" : "AllowStepFunctionsActions",
      "Action" : [
        "states:DescribeExecution",
        "states:GetExecutionHistory",
        "states:StartExecution",
        "states:StopExecution",
        "states:UpdateStateMachine"
      ],
      "Resource" : [
        "arn:aws:states:*:*:statemachine:*sagemaker*",
        "arn:aws:states:*:*:execution:*sagemaker*:*"
      ],
      "Effect" : "Allow"
    },
    {
      "Sid" : "AllowSecretManagerActions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:CreateSecret",
        "secretsmanager:PutResourcePolicy"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:AmazonSageMaker-*"
      ]
    },
    {
      "Sid" : "AllowServiceCatalogProvisionProduct",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:ProvisionProduct"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowServiceCatalogTerminateUpdateProvisionProduct",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:TerminateProvisionedProduct",
        "servicecatalog:UpdateProvisionedProduct"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "servicecatalog:userLevel" : "self"
        }
      }
    },
    {
      "Sid" : "AllowS3ObjectActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObject",
        "s3:PutObject",
        "s3:PutObjectRetention",
        "s3:ReplicateObject",
        "s3:RestoreObject",
        "s3:GetBucketAcl",
        "s3:PutObjectAcl"
      ],
      "Resource" : [
        "arn:aws:s3:::SageMaker-DataZone*",
        "arn:aws:s3:::DataZone-SageMaker*",
        "arn:aws:s3:::Sagemaker-DataZone*",
        "arn:aws:s3:::DataZone-Sagemaker*",
        "arn:aws:s3:::sagemaker-datazone*",
        "arn:aws:s3:::datazone-sagemaker*",
        "arn:aws:s3:::amazon-datazone*"
      ]
    },
    {
      "Sid" : "AllowS3GetObjectWithSageMakerExistingObjectTag",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ],
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/SageMaker" : "true"
```

```
        }
      }
    },
    {
      "Sid" : "AllowS3GetObjectWithServiceCatalogProvisioningExistingObjectTag",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ],
      "Condition" : {
        "StringEquals" : {
          "s3:ExistingObjectTag/servicecatalog:provisioning" : "true"
        }
      }
    },
    {
      "Sid" : "AllowS3BucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketCors",
        "s3:PutBucketCors"
      ],
      "Resource" : [
        "arn:aws:s3:::SageMaker-DataZone*",
        "arn:aws:s3:::DataZone-SageMaker*",
        "arn:aws:s3:::Sagemaker-DataZone*",
        "arn:aws:s3:::DataZone-Sagemaker*",
        "arn:aws:s3:::sagemaker-datazone*",
        "arn:aws:s3:::datazone-sagemaker*",
        "arn:aws:s3:::amazon-datazone*"
      ]
    },
    {
      "Sid" : "ReadSageMakerJumpstartArtifacts",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : [
        "arn:aws:s3:::jumpstart-cache-prod-us-west-2/*",
```

```
        "arn:aws:s3:::jumpstart-cache-prod-us-east-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-us-east-2/*",
        "arn:aws:s3:::jumpstart-cache-prod-eu-west-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-eu-central-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-south-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-northeast-2/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-northeast-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-southeast-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-southeast-2/*"
      ]
    },
    {
      "Sid" : "AllowLambdaInvokeFunction",
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*SageMaker*",
        "arn:aws:lambda:*:*:function:*sagemaker*",
        "arn:aws:lambda:*:*:function:*Sagemaker*",
        "arn:aws:lambda:*:*:function:*LabelingFunction*"
      ]
    },
    {
      "Sid" : "AllowCreateServiceLinkedRoleForSageMakerApplicationAutoscaling",
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "sagemaker.application-autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowSNSActions",
      "Effect" : "Allow",
      "Action" : [
        "sns:Subscribe",
        "sns:CreateTopic",
        "sns:Publish"
      ],
```

```
      "Resource" : [
        "arn:aws:sns:*:*:*SageMaker*",
        "arn:aws:sns:*:*:*Sagemaker*",
        "arn:aws:sns:*:*:*sagemaker*"
      ]
    },
    {
      "Sid" : "AllowPassRoleForSageMakerRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/sm-provisioning/datazone_usr_sagemaker_execution_role_*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com",
            "bedrock.amazonaws.com",
            "states.amazonaws.com",
            "lakeformation.amazonaws.com",
            "events.amazonaws.com",
            "sagemaker.amazonaws.com",
            "forecast.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CrossAccountKmsOperations",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:Decrypt",
        "kms:ListKeys"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
```

```
    {
      "Sid" : "KmsOperationsWithResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:Decrypt",
        "kms:ListKeys",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:RetireGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "AllowAthenaActions",
      "Effect" : "Allow",
      "Action" : [
        "athena:BatchGetNamedQuery",
        "athena:BatchGetPreparedStatement",
        "athena:BatchGetQueryExecution",
        "athena:CreateNamedQuery",
        "athena:CreateNotebook",
        "athena:CreatePreparedStatement",
        "athena:CreatePresignedNotebookUrl",
        "athena:DeleteNamedQuery",
        "athena:DeleteNotebook",
        "athena:DeletePreparedStatement",
        "athena:ExportNotebook",
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetNamedQuery",
        "athena:GetPreparedStatement",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryResultsStream",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetTableMetadata",
        "athena:GetWorkGroup",
        "athena:ImportNotebook",
```

```
        "athena:ListDatabases",
        "athena:ListDataCatalogs",
        "athena:ListEngineVersions",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements",
        "athena:ListQueryExecutions",
        "athena:ListTableMetadata",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups",
        "athena:StartCalculationExecution",
        "athena:StartQueryExecution",
        "athena:StartSession",
        "athena:StopCalculationExecution",
        "athena:StopQueryExecution",
        "athena:TerminateSession",
        "athena:UpdateNamedQuery",
        "athena:UpdateNotebook",
        "athena:UpdateNotebookMetadata",
        "athena:UpdatePreparedStatement"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowGlueCreateDatabase",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/default"
      ]
    },
    {
      "Sid" : "AllowRedshiftGetClusterCredentials",
      "Effect" : "Allow",
      "Action" : [
        "redshift:GetClusterCredentials"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:dbuser:*/sagemaker_access*",
        "arn:aws:redshift:*:*:dbname:*"
```

```
      ]
    },
    {
      "Sid" : "AllowListTags",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:user-profile/*",
        "arn:aws:sagemaker:*:*:domain/*"
      ]
    },
    {
      "Sid" : "AllowCloudformationListStackResources",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStackResources"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/SC-*"
    },
    {
      "Sid" : "AllowGlueActions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:ListJobs",
        "glue:CreateSession",
        "glue:RunStatement",
        "glue:BatchCreatePartition",
        "glue:CreatePartitionIndex",
        "glue:CreateTable",
        "glue:BatchGetWorkflows",
        "glue:BatchUpdatePartition",
        "glue:BatchDeletePartition",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:UpdateTable",
        "glue:DeleteTableVersion",
        "glue:DeleteTable",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeletePartitionIndex",
```

```
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:BatchDeleteTableVersion",
        "glue:BatchDeleteTable",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:UpdatePartition",
        "glue:CreateBlueprint",
        "glue:CreateJob",
        "glue:CreateConnection",
        "glue:CreateCrawler",
        "glue:CreateDataQualityRuleset",
        "glue:CreateWorkflow",
        "glue:GetDatabases",
        "glue:GetTables",
        "glue:GetTable",
        "glue:SearchTables",
        "glue:NotifyEvent",
        "glue:ListSchemas",
        "glue:BatchGetJobs",
        "glue:GetConnection",
        "glue:GetDatabase"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowGlueActionsWithEnvironmentTag",
      "Effect" : "Allow",
      "Action" : [
        "glue:SearchTables",
        "glue:NotifyEvent",
        "glue:StartBlueprintRun",
        "glue:PutWorkflowRunProperties",
        "glue:StopCrawler",
        "glue:DeleteJob",
        "glue:DeleteWorkflow",
        "glue:UpdateCrawler",
        "glue:DeleteBlueprint",
        "glue:UpdateWorkflow",
        "glue:StartCrawler",
        "glue:ResetJobBookmark",
        "glue:UpdateJob",
```

```
        "glue:StartWorkflowRun",
        "glue:StopCrawlerSchedule",
        "glue:ResumeWorkflowRun",
        "glue:ListSchemas",
        "glue:DeleteCrawler",
        "glue:UpdateBlueprint",
        "glue:BatchStopJobRun",
        "glue:StopWorkflowRun",
        "glue:BatchGetJobs",
        "glue:BatchGetWorkflows",
        "glue:UpdateCrawlerSchedule",
        "glue:DeleteConnection",
        "glue:UpdateConnection",
        "glue:GetConnection",
        "glue:GetDatabase",
        "glue:GetTable",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:BatchDeleteConnection",
        "glue:StartCrawlerSchedule",
        "glue:StartJobRun",
        "glue:CreateWorkflow",
        "glue:*DataQuality*"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "AllowGlueDefaultAccess",
      "Effect" : "Allow",
      "Action" : [
        "glue:BatchGet*",
        "glue:Get*",
        "glue:SearchTables",
        "glue:List*",
        "glue:RunStatement"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/default",
```

```
        "arn:aws:glue:*:*:connection/dz-sm-*",
        "arn:aws:glue:*:*:session/*"
      ]
    },
    {
      "Sid" : "AllowRedshiftClusterActions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:GetClusterCredentialsWithIAM",
        "redshift:DescribeClusters"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:cluster:*",
        "arn:aws:redshift:*:*:dbname:*"
      ]
    },
    {
      "Sid" : "AllowCreateClusterUser",
      "Effect" : "Allow",
      "Action" : [
        "redshift:CreateClusterUser"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:dbuser:*"
      ]
    },
    {
      "Sid" : "AllowCreateSecretActions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AmazonDataZoneDomain" : "dzd*",
          "aws:RequestTag/AmazonDataZoneDomain" : "dzd*"
        },
        "Null" : {
          "aws:TagKeys" : "false",
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:ResourceTag/AmazonDataZoneDomain" : "false",
          "aws:RequestTag/AmazonDataZoneDomain" : "false",
```

```
          "aws:RequestTag/AmazonDataZoneProject" : "false"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneDomain",
            "AmazonDataZoneProject"
          ]
        }
      }
    },
    {
      "Sid" : "ForecastOperations",
      "Effect" : "Allow",
      "Action" : [
        "forecast:CreateExplainabilityExport",
        "forecast:CreateExplainability",
        "forecast:CreateForecastEndpoint",
        "forecast:CreateAutoPredictor",
        "forecast:CreateDatasetImportJob",
        "forecast:CreateDatasetGroup",
        "forecast:CreateDataset",
        "forecast:CreateForecast",
        "forecast:CreateForecastExportJob",
        "forecast:CreatePredictorBacktestExportJob",
        "forecast:CreatePredictor",
        "forecast:DescribeExplainabilityExport",
        "forecast:DescribeExplainability",
        "forecast:DescribeAutoPredictor",
        "forecast:DescribeForecastEndpoint",
        "forecast:DescribeDatasetImportJob",
        "forecast:DescribeDataset",
        "forecast:DescribeForecast",
        "forecast:DescribeForecastExportJob",
        "forecast:DescribePredictorBacktestExportJob",
        "forecast:GetAccuracyMetrics",
        "forecast:InvokeForecastEndpoint",
        "forecast:GetRecentForecastContext",
        "forecast:DescribePredictor",
        "forecast:TagResource",
        "forecast:DeleteResourceTree"
      ],
      "Resource" : [
        "arn:aws:forecast:*:*:*Canvas*"
      ]
```

```
    },
    {
      "Sid" : "RDSOperation",
      "Effect" : "Allow",
      "Action" : "rds:DescribeDBInstances",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowEventBridgeRule",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-data-prep-job" : "true"
        }
      }
    },
    {
      "Sid" : "EventBridgeOperations",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:PutTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sagemaker:is-canvas-data-prep-job" : "true"
        }
      }
    },
    {
      "Sid" : "EventBridgeTagBasedOperations",
      "Effect" : "Allow",
      "Action" : [
        "events:TagResource"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-data-prep-job" : "true",
```

```
          "aws:ResourceTag/sagemaker:is-canvas-data-prep-job" : "true"
        }
      }
    },
    {
      "Sid" : "EventBridgeListTagOperation",
      "Effect" : "Allow",
      "Action" : "events:ListTagsForResource",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowEMR",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListClusters"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSSOAction",
      "Effect" : "Allow",
      "Action" : [
        "sso:CreateApplicationAssignment",
        "sso:AssociateProfile"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DenyNotAction",
      "Effect" : "Deny",
      "NotAction" : [
        "sagemaker:*",
        "sagemaker-geospatial:*",
        "sqlworkbench:*",
        "datazone:*",
        "forecast:*",
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeleteScheduledAction",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
```

```
        "application-autoscaling:DescribeScheduledActions",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:PutScheduledAction",
        "application-autoscaling:RegisterScalableTarget",
        "athena:BatchGetNamedQuery",
        "athena:BatchGetPreparedStatement",
        "athena:BatchGetQueryExecution",
        "athena:CreateNamedQuery",
        "athena:CreateNotebook",
        "athena:CreatePreparedStatement",
        "athena:CreatePresignedNotebookUrl",
        "athena:DeleteNamedQuery",
        "athena:DeleteNotebook",
        "athena:DeletePreparedStatement",
        "athena:ExportNotebook",
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetNamedQuery",
        "athena:GetPreparedStatement",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryResultsStream",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetTableMetadata",
        "athena:GetWorkGroup",
        "athena:ImportNotebook",
        "athena:ListDatabases",
        "athena:ListDataCatalogs",
        "athena:ListEngineVersions",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements",
        "athena:ListQueryExecutions",
        "athena:ListTableMetadata",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups",
        "athena:StartCalculationExecution",
        "athena:StartQueryExecution",
        "athena:StartSession",
        "athena:StopCalculationExecution",
        "athena:StopQueryExecution",
        "athena:TerminateSession",
        "athena:UpdateNamedQuery",
        "athena:UpdateNotebook",
        "athena:UpdateNotebookMetadata",
```

```
        "athena:UpdatePreparedStatement",
        "aws-marketplace:ViewSubscriptions",
        "cloudformation:GetTemplateSummary",
        "cloudformation:ListStackResources",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:PutMetricData",
        "codebuild:BatchGetBuilds",
        "codebuild:StartBuild",
        "codecommit:BatchGetRepositories",
        "codecommit:CreateRepository",
        "codecommit:GetRepository",
        "codecommit:List*",
        "codecommit:GitPull",
        "codecommit:GitPush",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeVpcs",
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:CreateRepository",
        "ecr:Describe*",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer",
        "ecr:SetRepositoryPolicy",
        "ecr:CompleteLayerUpload",
        "ecr:BatchDeleteImage",
        "ecr:UploadLayerPart",
        "ecr:DeleteRepositoryPolicy",
        "ecr:InitiateLayerUpload",
        "ecr:DeleteRepository",
```

```
        "ecr:PutImage",
        "ecr:StartImageScan",
        "ecr:TagResource",
        "ecr:UntagResource",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListClusters",
        "events:PutRule",
        "events:DescribeRule",
        "events:PutTargets",
        "events:TagResource",
        "events:ListTagsForResource",
        "fsx:DescribeFileSystems",
        "glue:SearchTables",
        "glue:NotifyEvent",
        "glue:StartBlueprintRun",
        "glue:PutWorkflowRunProperties",
        "glue:StopCrawler",
        "glue:DeleteJob",
        "glue:DeleteWorkflow",
        "glue:UpdateCrawler",
        "glue:DeleteBlueprint",
        "glue:UpdateWorkflow",
        "glue:StartCrawler",
        "glue:ResetJobBookmark",
        "glue:UpdateJob",
        "glue:StartWorkflowRun",
        "glue:StopCrawlerSchedule",
        "glue:ResumeWorkflowRun",
        "glue:DeleteCrawler",
        "glue:UpdateBlueprint",
        "glue:BatchStopJobRun",
        "glue:StopWorkflowRun",
        "glue:BatchGet*",
        "glue:UpdateCrawlerSchedule",
        "glue:DeleteConnection",
        "glue:UpdateConnection",
        "glue:Get*",
        "glue:BatchDeleteConnection",
        "glue:StartCrawlerSchedule",
        "glue:StartJobRun",
        "glue:CreateWorkflow",
```

```
        "glue:*DataQuality*",
        "glue:List*",
        "glue:CreateSession",
        "glue:RunStatement",
        "glue:BatchCreatePartition",
        "glue:CreateDatabase",
        "glue:CreatePartitionIndex",
        "glue:CreateTable",
        "glue:BatchUpdatePartition",
        "glue:BatchDeletePartition",
        "glue:UpdateTable",
        "glue:DeleteTableVersion",
        "glue:DeleteTable",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeletePartitionIndex",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:BatchDeleteTableVersion",
        "glue:BatchDeleteTable",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:UpdatePartition",
        "glue:CreateBlueprint",
        "glue:CreateJob",
        "glue:CreateConnection",
        "glue:CreateCrawler",
        "groundtruthlabeling:*",
        "iam:CreateServiceLinkedRole",
        "iam:GetRole",
        "iam:ListRoles",
        "iam:PassRole",
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:Decrypt",
        "kms:ListKeys",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:RetireGrant",
        "lakeformation:GetDataAccess",
        "lambda:ListFunctions",
        "lambda:InvokeFunction",
        "logs:CreateLogDelivery",
        "logs:CreateLogGroup",
```

```
        "logs:CreateLogStream",
        "logs:DeleteLogDelivery",
        "logs:Describe*",
        "logs:GetLogDelivery",
        "logs:GetLogEvents",
        "logs:ListLogDeliveries",
        "logs:PutLogEvents",
        "logs:UpdateLogDelivery",
        "ram:AcceptResourceShareInvitation",
        "rds:DescribeDBInstances",
        "redshift:CreateClusterUser",
        "redshift:GetClusterCredentials",
        "redshift:GetClusterCredentialsWithIAM",
        "redshift:DescribeClusters",
        "redshift-data:BatchExecuteStatement",
        "redshift-data:CancelStatement",
        "redshift-data:DescribeStatement",
        "redshift-data:DescribeTable",
        "redshift-data:ExecuteStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:GetCredentials",
        "s3:GetBucketAcl",
        "s3:PutObjectAcl",
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:AbortMultipartUpload",
        "s3:CreateBucket",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketCors",
        "s3:PutBucketCors",
        "s3:DeleteObjectVersion",
        "s3:PutObjectRetention",
        "s3:ReplicateObject",
        "s3:RestoreObject",
        "secretsmanager:ListSecrets",
```

```
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:CreateSecret",
        "secretsmanager:PutResourcePolicy",
        "secretsmanager:TagResource",
        "servicecatalog:Describe*",
        "servicecatalog:List*",
        "servicecatalog:ScanProvisionedProducts",
        "servicecatalog:SearchProducts",
        "servicecatalog:SearchProvisionedProducts",
        "servicecatalog:ProvisionProduct",
        "servicecatalog:TerminateProvisionedProduct",
        "servicecatalog:UpdateProvisionedProduct",
        "sns:ListTopics",
        "sns:Subscribe",
        "sns:CreateTopic",
        "sns:Publish",
        "states:DescribeExecution",
        "states:GetExecutionHistory",
        "states:StartExecution",
        "states:StopExecution",
        "states:UpdateStateMachine",
        "tag:GetResources",
        "sso:CreateApplicationAssignment",
        "sso:AssociateProfile"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonDataZoneSageMakerManageAccessRolePolicy

説明: AmazonDataZoneSageMakerManageAccessRolePolicy ポリシーは、Amazon DataZone に SageMaker 環境のさまざまなリソースへのユーザーアクセスを許可するために必要な権限を付与します。

AmazonDataZoneSageMakerManageAccessRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDataZoneSageMakerManageAccessRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 4 月 23 日 23:34 UTC
- 編集日時: 2024 年 11 月 21 日 20:21 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDataZoneSageMakerManageAccessRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
        "sagemaker:ListModelPackages",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribeAlgorithm",
        "sagemaker:ListTags",
        "sagemaker:DescribeDomain",
        "sagemaker:GetModelPackageGroupPolicy",
        "sagemaker:Search"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonSageMakerTaggingPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags",
        "sagemaker:DeleteTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "sagemaker:shared-with:*"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerModelPackageGroupPolicyPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:PutModelPackageGroupPolicy",
        "sagemaker:DeleteModelPackageGroupPolicy"
      ],
      "Resource" : [
        "arn:*:sagemaker:*:*:model-package-group/*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerRAMPermission",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShares",
        "ram:GetResourceShareInvitations",
```

```
        "ram:GetResourceShareAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonSageMakerRAMResourcePolicyPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:PutResourcePolicy",
        "sagemaker:GetResourcePolicy",
        "sagemaker:DeleteResourcePolicy"
      ],
      "Resource" : [
        "arn:*:sagemaker:*:*:feature-group/*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerRAMTagResourceSharePermission",
      "Effect" : "Allow",
      "Action" : [
        "ram:TagResource"
      ],
      "Resource" : "arn:*:ram:*:*:resource-share/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AwsDataZoneDomainId" : "false"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerRAMDeleteResourceSharePermission",
      "Effect" : "Allow",
      "Action" : [
        "ram:DeleteResourceShare"
      ],
      "Resource" : "arn:*:ram:*:*:resource-share/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AwsDataZoneDomainId" : "false"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerRAMCreateResourceSharePermission",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "ram:RequestedResourceType" : [
            "sagemaker:*"
          ]
        },
        "Null" : {
          "aws:RequestTag/AwsDataZoneDomainId" : "false"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerS3BucketPolicyPermission",
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteBucketPolicy",
        "s3:PutBucketPolicy",
        "s3:GetBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-datazone*",
        "arn:aws:s3:::SageMaker-DataZone*",
        "arn:aws:s3:::datazone-sagemaker*",
        "arn:aws:s3:::DataZone-SageMaker*",
        "arn:aws:s3:::amazon-datazone*",
        "arn:aws:s3:::amazon-sagemaker*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerS3Permission",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-datazone*",
        "arn:aws:s3:::SageMaker-DataZone*",
        "arn:aws:s3:::datazone-sagemaker*",
```

```
        "arn:aws:s3:::DataZone-SageMaker*",
        "arn:aws:s3:::amazon-datazone*",
        "arn:aws:s3:::amazon-sagemaker*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerECRPermission",
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetRepositoryPolicy",
        "ecr:SetRepositoryPolicy",
        "ecr:DeleteRepositoryPolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerKMSReadPermission",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneEnvironment"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerKMSGrantPermission",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
```

```
          "aws:TagKeys" : [
            "AmazonDataZoneEnvironment"
          ]
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonDataZoneSageMakerProvisioningRolePolicy

説明: AmazonDataZoneSageMakerProvisioningRolePolicy ポリシーは、Amazon DataZone に Amazon SageMaker との相互運用に必要なアクセス許可を付与します。

`AmazonDataZoneSageMakerProvisioningRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonDataZoneSageMakerProvisioningRolePolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 4 月 23 日 23:32 UTC
- 編集日時: 2025 年 1 月 9 日 20:52 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateSageMakerStudio",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateDomain"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneEnvironment"
          ]
        },
        "Null" : {
          "aws:TagKeys" : "false",
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false",
          "aws:RequestTag/AmazonDataZoneEnvironment" : "false"
        }
      }
```

```
    },
    {
      "Sid" : "DeleteSageMakerStudio",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DeleteDomain"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZoneEnvironment"
          ]
        },
        "Null" : {
          "aws:TagKeys" : "false",
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentSageMakerDescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeDomain"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "IamPassRolePermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/sm-provisioning/datazone_usr*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com",
            "lakeformation.amazonaws.com",
            "sagemaker.amazonaws.com"
          ],
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZonePermissionsToCreateEnvironmentRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:DetachRolePolicy",
        "iam:DeleteRolePolicy",
        "iam:AttachRolePolicy",
        "iam:PutRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/sm-provisioning/datazone_usr*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ],
          "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/
AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary"
        }
      }
    },
    {
```

```
      "Sid" : "AmazonDataZonePermissionsToManageEnvironmentRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:DeleteRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/sm-provisioning/datazone_usr*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZonePermissionsToCreateSageMakerServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/sagemaker.amazonaws.com/
AWSServiceRoleForAmazonSageMakerNotebooks"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentParameterValidation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "sagemaker:ListDomains"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentKMSKeyValidation",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentGluePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateConnection",
        "glue:DeleteConnection",
        "glue:GetConnection"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:connection/dz-sm-athena-glue-connection-*",
        "arn:aws:glue:*:*:connection/dz-sm-redshift-cluster-connection-*",
        "arn:aws:glue:*:*:connection/dz-sm-redshift-serverless-connection-*",
        "arn:aws:glue:*:*:catalog"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する

- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonDetectiveFullAccess

説明: Amazon Detective サービスへのフルアクセスと、コンソール UI の依存関係へのスコープ付きアクセスを提供します。

AmazonDetectiveFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDetectiveFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 4 月 30 日 17:57 UTC
- 編集日時: 2023 年 5 月 17 日 19:39 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDetectiveFullAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonDetectiveInvestigatorAccess

説明: 調査員による Amazon Detective サービスへのアクセスと、コンソール UI の依存関係へのスコープ付きアクセスを提供します。このポリシーでは、調査目的で Detective に掘り下げるアクセス許可と、Guardduty への制限付き書き込みアクセス許可を付与します。

AmazonDetectiveInvestigatorAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDetectiveInvestigatorAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 1 月 17 日 15:24 UTC
- 編集日時: 2023 年 11 月 27 日 03:13 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDetectiveInvestigatorAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonDetectiveMemberAccess

説明: Amazon Detective サービスへのメンバーアクセスと、コンソール UI の依存関係へのスコープ付きアクセスを提供します。

`AmazonDetectiveMemberAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonDetectiveMemberAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 1 月 17 日 15:16 UTC
- 編集日時: 2023 年 1 月 17 日 15:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDetectiveMemberAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonDetectiveOrganizationsAccess

説明: Amazon Detective の委任管理者を管理するための Organizations アクセスと、コンソール UI の依存関係へのスコープ付きアクセスを提供します。これにより、Detective のサービスリンクロールを作成するアクセス許可も付与されます。

AmazonDetectiveOrganizationsAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDetectiveOrganizationsAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 3 月 2 日 15:20 UTC
- 編集日時: 2023 年 3 月 2 日 15:20 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDetectiveOrganizationsAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonDetectiveServiceLinkedRolePolicy

説明: Amazon Detective がユーザーに代わってサービスコールを実行することを許可します

AmazonDetectiveServiceLinkedRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 11 月 18 日 19:47 UTC
- 編集日時: 2021 年 11 月 18 日 19:47 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonDetectiveServiceLinkedRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonDevOpsGuruConsoleFullAccess

説明: ポリシーでは、DevOps Guru コンソールへのフルアクセスを付与します。

AmazonDevOpsGuruConsoleFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDevOpsGuruConsoleFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 12 月 17 日 18:43 UTC
- 編集日時: 2022 年 8 月 25 日 18:18 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDevOpsGuruConsoleFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonDevOpsGuruFullAccess

説明: Amazon DevOps Guru へのフルアクセスを提供します。

AmazonDevOpsGuruFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDevOpsGuruFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 12 月 1 日 16:38 UTC
- 編集日時: 2022 年 8 月 25 日 18:23 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDevOpsGuruFullAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonDevOpsGuruOrganizationsAccess

説明: 組織内の Amazon DevOps Guru を有効化および管理するためのアクセスを提供します。

AmazonDevOpsGuruOrganizationsAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDevOpsGuruOrganizationsAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 11 月 15 日 23:50 UTC
- 編集日時: 2021 年 11 月 15 日 23:50 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDevOpsGuruOrganizationsAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonDevOpsGuruReadOnlyAccess

説明: Amazon DevOps Guru コンソールへの読み取り専用アクセスを提供します。

AmazonDevOpsGuruReadOnlyAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDevOpsGuruReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 12 月 1 日 16:34 UTC
- 編集日時: 2022 年 8 月 25 日 18:11 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDevOpsGuruReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonDevOpsGuruServiceRolePolicy

説明: Amazon DevOpsGuru がリソースにアクセスする際に必要となるサービスリンクロール。

`AmazonDevOpsGuruServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 12 月 1 日 10:24 UTC
- 編集日時: 2023 年 1 月 10 日 14:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonDevOpsGuruServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v9 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonDMSCloudWatchLogsRole

説明: DMS レプリケーションログを顧客アカウントの Cloudwatch ログにアップロードするためのアクセスを提供します。

AmazonDMSCloudWatchLogsRole は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDMSCloudWatchLogsRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2016 年 1 月 7 日 23:44 UTC
- 編集日時: 2023 年 5 月 23 日 21:32 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDMSCloudWatchLogsRole`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonDMSRedshiftS3Role

説明: DMS の Redshift エンドポイントの S3 設定を管理するためのアクセスを提供します。

AmazonDMSRedshiftS3Role は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDMSRedshiftS3Role をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2016 年 4 月 20 日 17:05 UTC
- 編集日時: 2019 年 7 月 8 日 18:19 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonDMSRedshiftS3Role

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonDMSVPCManagementRole

説明: AWS マネージド型顧客設定の VPC 設定を管理するためのアクセスを提供します

AmazonDMSVPCManagementRole は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDMSVPCManagementRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 11 月 18 日 16:33 UTC

- 編集日時: 2024 年 7 月 25 日 15:19 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonDMSVPCManagementRole

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Statement1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonDocDB-ElasticServiceRolePolicy

説明: Amazon DocumentDB-Elastic がユーザーに代わって AWS リソースを管理できるようにします。

AmazonDocDB-ElasticServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 11 月 30 日 14:17 UTC
- 編集日時: 2022 年 11 月 30 日 14:17 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonDocDB-ElasticServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonDocDBConsoleFullAccess

説明: AWS マネジメントコンソールを使用して Amazon DocumentDB (MongoDB 互換) を管理するためのフルアクセスを提供します。このポリシーは、アカウント内のすべての SNS トピックを公開するためのフルアクセス、Amazon EC2 インスタンスと VPC 設定を作成および編集するアクセス許可、Amazon KMS でキーを表示および一覧表示するアクセス許可、Amazon RDS と Amazon Neptune へのフルアクセス権も付与します。

`AmazonDocDBConsoleFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonDocDBConsoleFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 1 月 9 日 20:37 UTC
- 編集日時: 2025 年 2 月 11 日 18:22 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DocdbSids",
      "Effect" : "Allow",
      "Action" : [
        "docdb-elastic:CreateCluster",
        "docdb-elastic:UpdateCluster",
        "docdb-elastic:GetCluster",
        "docdb-elastic:DeleteCluster",
        "docdb-elastic:ListClusters",
        "docdb-elastic:CreateClusterSnapshot",
        "docdb-elastic:GetClusterSnapshot",
        "docdb-elastic:DeleteClusterSnapshot",
        "docdb-elastic:ListClusterSnapshots",
        "docdb-elastic:RestoreClusterFromSnapshot",
        "docdb-elastic:TagResource",
        "docdb-elastic:UntagResource",
        "docdb-elastic:ListTagsForResource",
        "docdb-elastic:CopyClusterSnapshot",
        "docdb-elastic:StartCluster",
        "docdb-elastic:StopCluster",
        "docdb-elastic:GetPendingMaintenanceAction",
        "docdb-elastic:ListPendingMaintenanceActions",
        "docdb-elastic:ApplyPendingMaintenanceAction",
        "rds:AddRoleToDBCluster",
        "rds:AddSourceIdentifierToSubscription",
        "rds:AddTagsToResource",
        "rds:ApplyPendingMaintenanceAction",
```

```
        "rds:CopyDBClusterParameterGroup",
        "rds:CopyDBClusterSnapshot",
        "rds:CopyDBParameterGroup",
        "rds:CreateDBCluster",
        "rds:CreateDBClusterParameterGroup",
        "rds:CreateDBClusterSnapshot",
        "rds:CreateDBInstance",
        "rds:CreateDBParameterGroup",
        "rds:CreateDBSubnetGroup",
        "rds:CreateEventSubscription",
        "rds:CreateGlobalCluster",
        "rds:DeleteDBCluster",
        "rds:DeleteDBClusterParameterGroup",
        "rds:DeleteDBClusterSnapshot",
        "rds:DeleteDBInstance",
        "rds:DeleteDBParameterGroup",
        "rds:DeleteDBSubnetGroup",
        "rds:DeleteEventSubscription",
        "rds:DeleteGlobalCluster",
        "rds:DescribeAccountAttributes",
        "rds:DescribeCertificates",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBLogFiles",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultClusterParameters",
        "rds:DescribeEngineDefaultParameters",
        "rds:DescribeEventCategories",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeEvents",
        "rds:DescribeGlobalClusters",
        "rds:DescribeOptionGroups",
        "rds:DescribeOrderableDBInstanceOptions",
        "rds:DescribePendingMaintenanceActions",
        "rds:DescribeValidDBInstanceModifications",
        "rds:DownloadDBLogFilePortion",
```

```
        "rds:FailoverDBCluster",
        "rds:ListTagsForResource",
        "rds:ModifyDBCluster",
        "rds:ModifyDBClusterParameterGroup",
        "rds:ModifyDBClusterSnapshotAttribute",
        "rds:ModifyDBInstance",
        "rds:ModifyDBParameterGroup",
        "rds:ModifyDBSubnetGroup",
        "rds:ModifyEventSubscription",
        "rds:ModifyGlobalCluster",
        "rds:PromoteReadReplicaDBCluster",
        "rds:RebootDBInstance",
        "rds:RemoveFromGlobalCluster",
        "rds:RemoveRoleFromDBCluster",
        "rds:RemoveSourceIdentifierFromSubscription",
        "rds:RemoveTagsFromResource",
        "rds:ResetDBClusterParameterGroup",
        "rds:ResetDBParameterGroup",
        "rds:RestoreDBClusterFromSnapshot",
        "rds:RestoreDBClusterToPointInTime"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DependencySids",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "ec2:AllocateAddress",
        "ec2:AssignIpv6Addresses",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssociateAddress",
        "ec2:AssociateRouteTable",
        "ec2:AssociateSubnetCidrBlock",
        "ec2:AssociateVpcCidrBlock",
        "ec2:AttachInternetGateway",
        "ec2:AttachNetworkInterface",
        "ec2:CreateCustomerGateway",
        "ec2:CreateDefaultSubnet",
```

```
        "ec2:CreateDefaultVpc",
        "ec2:CreateInternetGateway",
        "ec2:CreateNatGateway",
        "ec2:CreateNetworkInterface",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateVpc",
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupReferences",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:ModifyVpcEndpoint",
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListKeyPolicies",
        "kms:ListKeys",
        "kms:ListRetirableGrants",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "sns:ListSubscriptions",
        "sns:ListTopics",
        "sns:Publish"
      ],
      "Resource" : [
        "*"
      ]
    },
```

```
    {
      "Sid" : "DocdbSLRSid",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/rds.amazonaws.com/
AWSServiceRoleForRDS",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "rds.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DocdbElasticSLRSid",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/docdb-elastic.amazonaws.com/
AWSServiceRoleForDocDB-Elastic",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "docdb-elastic.amazonaws.com"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonDocDBElasticFullAccess

説明: Amazon DocumentDB Elastic クラスターへのフルアクセス
と、EC2、KMS、SecretsManager、CloudWatch、IAM などの依存関係に必要なその他のアクセス許可を提供します。

AmazonDocDBElasticFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDocDBElasticFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 6 月 5 日 13:51 UTC
- 編集日時: 2025 年 2 月 11 日 18:22 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDocDBElasticFullAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
        "docdb-elastic:TagResource",
        "docdb-elastic:UntagResource",
        "docdb-elastic:ListTagsForResource",
        "docdb-elastic:CopyClusterSnapshot",
        "docdb-elastic:StartCluster",
        "docdb-elastic:StopCluster",
        "docdb-elastic:GetPendingMaintenanceAction",
        "docdb-elastic:ListPendingMaintenanceActions",
        "docdb-elastic:ApplyPendingMaintenanceAction"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EC2Sid",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeVpcEndpoints",
        "ec2:DeleteVpcEndpoints",
        "ec2:ModifyVpcEndpoint",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeAvailabilityZones",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "docdb-elastic.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "KMSSid",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:DescribeKey",
```

```
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "docdb-elastic.*.amazonaws.com"
          ],
          "aws:ResourceTag/DocDBElasticFullAccess" : "*"
        }
      }
    },
    {
      "Sid" : "KMSGrantSid",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/DocDBElasticFullAccess" : "*",
          "kms:ViaService" : [
            "docdb-elastic.*.amazonaws.com"
          ]
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        }
      }
    },
    {
      "Sid" : "SecretManagerSid",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:ListSecretVersionIds",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:GetResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:ResourceTag/DocDBElasticFullAccess" : "*"
```

```
        },
        "StringEquals" : {
          "aws:CalledViaFirst" : "docdb-elastic.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudwatchSid",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SLRSid",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/docdb-elastic.amazonaws.com/
AWSServiceRoleForDocDB-Elastic",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "docdb-elastic.amazonaws.com"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonDocDBElasticReadOnlyAccess

説明: Amazon DocDB-Elastic と CloudWatch メトリクスへの読み取りアクセスを提供します。

AmazonDocDBElasticReadOnlyAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDocDBElasticReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 6 月 8 日 14:37 UTC
- 編集日時: 2023 年 6 月 21 日 16:57 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDocDBElasticReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonDocDBFullAccess

説明: Amazon DocumentDB (MongoDB 互換) へのフルアクセスを提供します。このポリシーは、アカウント内のすべての SNS トピックを公開するためのフルアクセスと、Amazon RDS と Amazon Neptune へのフルアクセス権も付与します。

`AmazonDocDBFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonDocDBFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 1 月 9 日 20:21 UTC
- 編集日時: 2019 年 1 月 9 日 20:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonDocDBReadOnlyAccess

説明: Amazon DocumentDB (MongoDB 互換) への読み取り専用アクセスを提供します。このポリシーは Amazon RDS と Amazon Neptune リソースへのアクセス権も付与します。

AmazonDocDBReadOnlyAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDocDBReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 1 月 9 日 20:30 UTC
- 編集日時: 2019 年 1 月 9 日 20:30 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDocDBReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonDRSVPCManagement

説明: Amazon が管理する顧客設定の VPC 設定を管理するためのアクセスを提供します

AmazonDRSVPCManagement は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDRSVPCManagement をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 9 月 2 日 00:09 UTC

- 編集日時: 2015 年 9 月 2 日 00:09 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDRSVPCManagement`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する

- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonDynamoDBFullAccess

説明: 経由で Amazon DynamoDB へのフルアクセスを提供します AWS マネジメントコンソール。

AmazonDynamoDBFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDynamoDBFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2021 年 1 月 29 日 17:38 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDynamoDBFullAccess

ポリシーのバージョン

ポリシーのバージョン: v15 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonDynamoDBFullAccess_v2

説明: Amazon DynamoDB へのフルアクセスを提供します。

AmazonDynamoDBFullAccess_v2 は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDynamoDBFullAccess_v2 をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 5 月 22 日 14:52 UTC
- 編集日時: 2025 年 5 月 22 日 14:52 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDynamoDBFullAccess_v2

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DDBAndDAXFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:*",
        "dax:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSIntegration",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LambdaIntegration",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListEventSourceMappings",
        "lambda:ListFunctions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DaxSNSIntegration",
      "Effect" : "Allow",
```

```
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ApplicationAutoscalingIntegration",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "application-autoscaling:service-namespace" : "dynamodb"
        }
      }
    },
    {
      "Sid" : "ApplicationAutoscalingDescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TagManagement",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudwatchMonitoring",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
```

```
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListKinesisResources",
      "Effect" : "Allow",
      "Action" : [
        "kinesis:ListStreams",
        "kinesis:DescribeStream",
        "kinesis:DescribeStreamSummary"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListEC2ResourcesForDaxClusterCreation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudwatchInsightsRules",
      "Effect" : "Allow",
      "Action" : "cloudwatch:GetInsightRuleReport",
      "Resource" : "arn:aws:cloudwatch:*:*:insight-rule/DynamoDBContributorInsights*"
    },
    {
      "Sid" : "ServiceRoleCreation",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "replication.dynamodb.amazonaws.com",
            "dax.amazonaws.com",
            "dynamodb.application-autoscaling.amazonaws.com",
```

```
            "contributorinsights.dynamodb.amazonaws.com",
            "kinesisreplication.dynamodb.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "IamIntegration",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonDynamoDBFullAccesswithDataPipeline

説明: このポリシーは非推奨化される予定です。ガイダンスについては、「https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/DynamoDBPipeline.html」のドキュメントを参照してください。経由で AWS Data Pipeline を使用したエクスポート/インポートを含む Amazon DynamoDB へのフルアクセスを提供します AWS マネジメントコンソール。

`AmazonDynamoDBFullAccesswithDataPipeline` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonDynamoDBFullAccesswithDataPipeline` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2015 年 11 月 12 日 02:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDynamoDBFullAccesswithDataPipeline`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonDynamoDBReadOnlyAccess

説明: 経由で Amazon DynamoDB への読み取り専用アクセスを提供します AWS マネジメントコンソール。

`AmazonDynamoDBReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonDynamoDBReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2024 年 11 月 18 日 17:38 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDynamoDBReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v15 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GeneralReadOnlyAccess",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricData",
        "datapipeline:DescribeObjects",
        "datapipeline:DescribePipelines",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:ListPipelines",
        "datapipeline:QueryObjects",
        "dynamodb:BatchGetItem",
        "dynamodb:Describe*",
        "dynamodb:List*",
        "dynamodb:GetAbacStatus",
        "dynamodb:GetItem",
        "dynamodb:GetResourcePolicy",
        "dynamodb:Query",
```

```
        "dynamodb:Scan",
        "dynamodb:PartiQLSelect",
        "dax:Describe*",
        "dax:List*",
        "dax:GetItem",
        "dax:BatchGetItem",
        "dax:Query",
        "dax:Scan",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "iam:GetRole",
        "iam:ListRoles",
        "kms:DescribeKey",
        "kms:ListAliases",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "lambda:ListFunctions",
        "lambda:ListEventSourceMappings",
        "lambda:GetFunctionConfiguration",
        "resource-groups:ListGroups",
        "resource-groups:ListGroupResources",
        "resource-groups:GetGroup",
        "resource-groups:GetGroupQuery",
        "tag:GetResources",
        "kinesis:ListStreams",
        "kinesis:DescribeStream",
        "kinesis:DescribeStreamSummary"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "CCIAccess",
      "Action" : "cloudwatch:GetInsightRuleReport",
      "Effect" : "Allow",
      "Resource" : "arn:aws:cloudwatch:*:*:insight-rule/DynamoDBContributorInsights*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonEBSCSIDriverPolicy

説明: CSI ドライバーサービスアカウントがユーザーに代わって EC2 などの関連サービスを呼び出すことを許可する IAM ポリシー。

AmazonEBSCSIDriverPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEBSCSIDriverPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 4 月 4 日 17:24 UTC
- 編集日時: 2025 年 11 月 17 日 17:04 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEBSCSIDriverPolicy

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshots",
        "ec2:DescribeTags",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeVolumeStatus"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot",
        "ec2:ModifyVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopyVolumes"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/vol-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateVolume",
        "ec2:EnableFastSnapshotRestores"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateVolume",
            "CreateSnapshot",
            "CopyVolumes"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume",
        "ec2:CopyVolumes"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
```

```
          "aws:RequestTag/ebs.csi.aws.com/cluster" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume",
        "ec2:CopyVolumes"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/CSIVolumeName" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/ebs.csi.aws.com/cluster" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/CSIVolumeName" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:DeleteVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/kubernetes.io/created-for/pvc/name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/CSIVolumeSnapshotName" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/ebs.csi.aws.com/cluster" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/CSIVolumeSnapshotName" : "*"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/ebs.csi.aws.com/cluster" : "true"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonEC2ContainerRegistryFullAccess

説明: Amazon ECR リソースへの管理アクセスを提供します

AmazonEC2ContainerRegistryFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEC2ContainerRegistryFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 12 月 21 日 17:06 UTC

- 編集日時: 2020 年 12 月 5 日 00:04 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryFullAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonEC2ContainerRegistryPowerUser

説明: Amazon EC2 Container Registry リポジトリへのフルアクセスを提供しますが、リポジトリの削除やポリシーの変更は許可されません。

`AmazonEC2ContainerRegistryPowerUser` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonEC2ContainerRegistryPowerUser` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 12 月 21 日 17:05 UTC
- 編集日時: 2019 年 12 月 10 日 20:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryPowerUser`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
```

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonEC2ContainerRegistryPullOnly

説明: Amazon EC2 Container Registry リポジトリからイメージをプルするためのアクセスを提供します。

`AmazonEC2ContainerRegistryPullOnly` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEC2ContainerRegistryPullOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 10 月 04 日 16:58 UTC
- 編集日時: 2024 年 10 月 04 日 16:58 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryPullOnly

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchGetImage",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchImportUpstreamImage"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonEC2ContainerRegistryReadOnly

説明: Amazon EC2 Container Registry リポジトリへの読み取り専用アクセスを提供します。

`AmazonEC2ContainerRegistryReadOnly` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonEC2ContainerRegistryReadOnly` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 12 月 21 日 17:04 UTC
- 編集日時: 2019 年 12 月 10 日 20:56 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryReadOnly`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonEC2ContainerServiceAutoscaleRole

説明: Amazon EC2 Container Service のタスク自動スケーリングを有効にするポリシー

AmazonEC2ContainerServiceAutoscaleRole は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEC2ContainerServiceAutoscaleRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2016 年 5 月 12 日 23:25 UTC
- 編集日時: 2018 年 2 月 5 日 19:15 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceAutoscaleRole`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeServices",
        "ecs:UpdateService"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : [
        "*"
      ]
```

```
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonEC2ContainerServiceEventsRole

説明: EC2 Container Service で CloudWatch Events を有効にするポリシー

`AmazonEC2ContainerServiceEventsRole` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonEC2ContainerServiceEventsRole` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2017 年 5 月 30 日 16:51 UTC
- 編集日時: 2023 年 3 月 6 日 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceEventsRole`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonEC2ContainerServiceforEC2Role

説明: Amazon EC2 Container Service の Amazon EC2 ロール向けデフォルトポリシー。

`AmazonEC2ContainerServiceforEC2Role` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonEC2ContainerServiceforEC2Role` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 3 月 19 日 18:45 UTC
- 編集日時: 2025 年 8 月 4 日 18:19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceforEC2Role`

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeTags",
        "ecs:CreateCluster",
        "ecs:DeregisterContainerInstance",
        "ecs:DiscoverPollEndpoint",
        "ecs:Poll",
        "ecs:RegisterContainerInstance",
        "ecs:StartTelemetrySession",
        "ecs:UpdateContainerInstancesState",
        "ecs:Submit*",
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ecs:TagResource",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ecs:CreateAction" : [
            "CreateCluster",
            "RegisterContainerInstance"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:task/*/*",
        "arn:aws:ecs:*:*:container-instance/*/*"
```

```
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonEC2ContainerServiceRole

説明: Amazon ECS サービスロールのデフォルトポリシー。

AmazonEC2ContainerServiceRole は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEC2ContainerServiceRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 4 月 9 日 16:14 UTC
- 編集日時: 2016 年 8 月 11 日 13:08 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceRole

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:Describe*",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:Describe*",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:RegisterTargets"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonEC2FullAccess

説明: 経由で Amazon EC2 へのフルアクセスを提供します AWS マネジメントコンソール。

`AmazonEC2FullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonEC2FullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2018 年 11 月 27 日 02:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2FullAccess`

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonEC2ImageReferencesAccessPolicy

説明: DescribeImageReferences を使用するときに、サポートされているすべてのリソースタイプをスキャンして関連データを検索するための読み取り専用アクセスを提供します。

AmazonEC2ImageReferencesAccessPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEC2ImageReferencesAccessPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 8 月 26 日 19:19 UTC
- 編集日時: 2025 年 8 月 26 日 19:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ImageReferencesAccessPolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "ec2:DescribeImageReferences",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeLaunchTemplateVersions",
        "ssm:DescribeParameters",
        "ssm:GetParameters",
        "imagebuilder:ListImageRecipes",
        "imagebuilder:ListContainerRecipes",
        "imagebuilder:GetContainerRecipe"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
```

```
          "aws:CalledVia" : [
            "ec2-images.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonEC2ReadOnlyAccess

説明: 経由で Amazon EC2 への読み取り専用アクセスを提供します AWS マネジメントコンソール。

`AmazonEC2ReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonEC2ReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2024 年 12 月 27 日 10:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:Describe*",
        "ec2:GetSecurityGroupsForVpc"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:Describe*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "autoscaling:Describe*",
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する

- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonEC2RoleforAWSCodeDeploy

説明: S3 バケットへの EC2 アクセスを提供し、リビジョンをダウンロードします。EC2 インスタンスの CodeDeploy エージェントには、このロールが必要です。

AmazonEC2RoleforAWSCodeDeploy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEC2RoleforAWSCodeDeploy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 5 月 19 日 18:10 UTC
- 編集日時: 2017 年 3 月 20 日 17:14 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforAWSCodeDeploy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonEC2RoleforAWSCodeDeployLimited

説明: リビジョンをダウンロードするための S3 バケットへの制限付きアクセスを EC2 に提供します。EC2 インスタンスの CodeDeploy エージェントには、このロールが必要です。

`AmazonEC2RoleforAWSCodeDeployLimited` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonEC2RoleforAWSCodeDeployLimited` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 8 月 24 日 17:55 UTC
- 編集日時: 2022 年 1 月 20 日 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforAWSCodeDeployLimited`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonEC2RoleforDataPipelineRole

説明: Amazon EC2 ロール Data Pipeline サービスロールのデフォルトポリシー。

AmazonEC2RoleforDataPipelineRole は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEC2RoleforDataPipelineRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2016 年 2 月 22 日 17:24 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforDataPipelineRole

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonEC2RoleforSSM

説明: このポリシーは間もなく廃止されます。AmazonSSMManagedInstanceCore ポリシーを使用して、EC2 インスタンスで AWS Systems Manager サービスコア機能を有効にしてください。詳細は、「https://docs.aws.amazon.com/systems-manager/latest/userguide/setup-instance-profile.html」を参照してください。

AmazonEC2RoleforSSM は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEC2RoleforSSM をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 5 月 29 日 17:48 UTC
- 編集日時: 2019 年 1 月 24 日 19:20 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforSSM

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonEC2RolePolicyForLaunchWizard

説明: EC2 の Amazon LaunchWizard サービスロールのマネージドポリシー

AmazonEC2RolePolicyForLaunchWizard は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEC2RolePolicyForLaunchWizard をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 11 月 13 日 08:05 UTC
- 編集日時: 2024 年 9 月 25 日 22:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEC2RolePolicyForLaunchWizard

ポリシーのバージョン

ポリシーのバージョン: v11 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:RebootInstances",
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/LaunchWizardResourceGroupID" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ReplaceRoute"
      ],
      "Resource" : "arn:aws:ec2:*:*:route-table/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/LaunchWizardApplicationType" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAddresses",
        "ec2:AssociateAddress",
        "ec2:DescribeInstances",
        "ec2:DescribeImages",
        "ec2:DescribeRegions",
        "ec2:DescribeVolumes",
        "ec2:DescribeRouteTables",
        "ec2:ModifyInstanceAttribute",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:PutMetricData",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:CreateVolume"
      ],
```

```
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "LaunchWizardResourceGroupID",
            "LaunchWizardApplicationType"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutObjectTagging",
        "s3:GetBucketLocation",
        "logs:PutLogEvents",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:*",
        "arn:aws:s3:::launchwizard*",
        "arn:aws:s3:::aws-sap-data-provider/config.properties"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:Create*",
      "Resource" : "arn:aws:logs:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:Describe*",
        "cloudformation:DescribeStackResources",
        "cloudformation:SignalResource",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "LaunchWizardResourceGroupID"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:BatchGetItem",
        "dynamodb:PutItem",
        "sqs:ReceiveMessage",
        "sqs:SendMessage",
        "dynamodb:Scan",
        "s3:ListBucket",
        "dynamodb:Query",
        "dynamodb:UpdateItem",
        "dynamodb:DeleteTable",
        "dynamodb:CreateTable",
        "s3:GetObject",
        "dynamodb:DescribeTable",
        "s3:GetBucketLocation",
        "dynamodb:UpdateTable"
      ],
      "Resource" : [
        "arn:aws:s3:::launchwizard*",
        "arn:aws:dynamodb:*:*:table/LaunchWizard*",
        "arn:aws:sqs:*:*:LaunchWizard*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ssm:resourceTag/LaunchWizardApplicationType" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:GetDocument"
```

```
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSSAP-InstallBackint",
        "arn:aws:ssm:*:*:document/AWSSAP-InstallBackintForAWSBackup"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeFileSystems",
        "fsx:ListTagsForResource",
        "fsx:DescribeStorageVirtualMachines"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "LaunchWizard*"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonEC2SpotFleetAutoscaleRole

説明: Amazon EC2 スポットフリートの自動スケーリングを有効にするポリシー

AmazonEC2SpotFleetAutoscaleRole は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEC2SpotFleetAutoscaleRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2016 年 8 月 19 日 18:27 UTC
- 編集日時: 2019 年 2 月 18 日 19:17 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2SpotFleetAutoscaleRole

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonEC2SpotFleetTaggingRole

説明: EC2 スポットフリートがお客様に代わってスポットインスタンスをリクエスト、終了、タグ付けできるようにします。

AmazonEC2SpotFleetTaggingRole は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEC2SpotFleetTaggingRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2017 年 6 月 29 日 18:19 UTC
- 編集日時: 2020 年 4 月 23 日 19:30 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2SpotFleetTaggingRole

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonECS_FullAccess

説明: Amazon ECS リソースへの管理アクセスを提供し、VPCs、Auto Scaling グループ、CloudFormation スタックなどの他の AWS サービスリソースへのアクセスを通じて ECS 機能を有効にします。

`AmazonECS_FullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonECS_FullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 11 月 7 日 21:36 UTC
- 編集日時: 2024 年 8 月 13 日 19:39 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonECS_FullAccess`

ポリシーのバージョン

ポリシーのバージョン: v21 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ECSIntegrationsManagementPolicy",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget",
        "appmesh:DescribeVirtualGateway",
        "appmesh:DescribeVirtualNode",
        "appmesh:ListMeshes",
        "appmesh:ListVirtualGateways",
        "appmesh:ListVirtualNodes",
        "autoscaling:CreateAutoScalingGroup",
        "autoscaling:CreateLaunchConfiguration",
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:DeleteLaunchConfiguration",
```

```
        "autoscaling:Describe*",
        "autoscaling:UpdateAutoScalingGroup",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStack*",
        "cloudformation:UpdateStack",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:PutMetricAlarm",
        "codedeploy:BatchGetApplicationRevisions",
        "codedeploy:BatchGetApplications",
        "codedeploy:BatchGetDeploymentGroups",
        "codedeploy:BatchGetDeployments",
        "codedeploy:ContinueDeployment",
        "codedeploy:CreateApplication",
        "codedeploy:CreateDeployment",
        "codedeploy:CreateDeploymentGroup",
        "codedeploy:GetApplication",
        "codedeploy:GetApplicationRevision",
        "codedeploy:GetDeployment",
        "codedeploy:GetDeploymentConfig",
        "codedeploy:GetDeploymentGroup",
        "codedeploy:GetDeploymentTarget",
        "codedeploy:ListApplicationRevisions",
        "codedeploy:ListApplications",
        "codedeploy:ListDeploymentConfigs",
        "codedeploy:ListDeploymentGroups",
        "codedeploy:ListDeployments",
        "codedeploy:ListDeploymentTargets",
        "codedeploy:RegisterApplicationRevision",
        "codedeploy:StopDeployment",
        "ec2:AssociateRouteTable",
        "ec2:AttachInternetGateway",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CancelSpotFleetRequests",
        "ec2:CreateInternetGateway",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateVpc",
        "ec2:DeleteLaunchTemplate",
```

```
        "ec2:DeleteSubnet",
        "ec2:DeleteVpc",
        "ec2:Describe*",
        "ec2:DetachInternetGateway",
        "ec2:DisassociateRouteTable",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:RequestSpotFleet",
        "ec2:RunInstances",
        "ecs:*",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeFileSystems",
        "elasticloadbalancing:CreateListener",
        "elasticloadbalancing:CreateLoadBalancer",
        "elasticloadbalancing:CreateRule",
        "elasticloadbalancing:CreateTargetGroup",
        "elasticloadbalancing:DeleteListener",
        "elasticloadbalancing:DeleteLoadBalancer",
        "elasticloadbalancing:DeleteRule",
        "elasticloadbalancing:DeleteTargetGroup",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTargetGroups",
        "events:DeleteRule",
        "events:DescribeRule",
        "events:ListRuleNamesByTarget",
        "events:ListTargetsByRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets",
        "fsx:DescribeFileSystems",
        "iam:ListAttachedRolePolicies",
        "iam:ListInstanceProfiles",
        "iam:ListRoles",
        "lambda:ListFunctions",
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups",
        "logs:FilterLogEvents",
        "route53:CreateHostedZone",
        "route53:DeleteHostedZone",
        "route53:GetHealthCheck",
        "route53:GetHostedZone",
        "route53:ListHostedZonesByName",
```

```
        "servicediscovery:CreatePrivateDnsNamespace",
        "servicediscovery:CreateService",
        "servicediscovery:DeleteService",
        "servicediscovery:GetNamespace",
        "servicediscovery:GetOperation",
        "servicediscovery:GetService",
        "servicediscovery:ListNamespaces",
        "servicediscovery:ListServices",
        "servicediscovery:UpdateService",
        "sns:ListTopics"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SSMPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:GetParameters",
        "ssm:GetParametersByPath"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/aws/service/ecs*"
    },
    {
      "Sid" : "ManagedCloudformationResourcesCleanupPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteInternetGateway",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-name" : "EC2ContainerService-*"
        }
      }
    },
    {
```

```
      "Sid" : "TasksPassRolePolicy",
      "Action" : "iam:PassRole",
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ecs-tasks.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "InfrastructurePassRolePolicy",
      "Action" : "iam:PassRole",
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/ecsInfrastructureRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ecs.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "InstancePassRolePolicy",
      "Action" : "iam:PassRole",
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/ecsInstanceRole*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Sid" : "AutoScalingPassRolePolicy",
      "Action" : "iam:PassRole",
```

```
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/ecsAutoscaleRole*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "application-autoscaling.amazonaws.com",
            "application-autoscaling.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Sid" : "ServiceLinkedRoleCreationPolicy",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : [
            "ecs.amazonaws.com",
            "autoscaling.amazonaws.com",
            "ecs.application-autoscaling.amazonaws.com",
            "spot.amazonaws.com",
            "spotfleet.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ELBTaggingPolicy",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "elasticloadbalancing:CreateAction" : [
            "CreateTargetGroup",
            "CreateRule",
            "CreateListener",
            "CreateLoadBalancer"
```

```
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonECSComputeServiceRolePolicy

説明: Amazon ECS Compute が ECS マネージドインスタンスの一部として EC2 インスタンスと関連リソースを管理できるようにするポリシー

`AmazonECSComputeServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2025 年 3 月 24 日 17:37 UTC
- 編集日時: 2025 年 3 月 28 日 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonECSComputeServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadOnlyPermissionsForInstanceManagement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeFleets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ReadOnlyPermissionsForInstanceEventWindows",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceEventWindows"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ReadOnlyPermissionsForLaunchTemplates",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeLaunchTemplateVersions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DeleteManagedLaunchTemplate",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ManagedResourceOperator" : "ecs.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "TerminateManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ManagedResourceOperator" : "ecs.amazonaws.com"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonECSInfrastructureRoleforExpressGatewayServices

説明: これらのアクセス許可により、Amazon ECS はロードバランシング、セキュリティグループ、SSL 証明書、自動スケーリング設定など、Express Gateway サービスに必要なインフラストラクチャコンポーネントを自動的にプロビジョニングおよび管理できます。

AmazonECSInfrastructureRoleforExpressGatewayServices は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonECSInfrastructureRoleforExpressGatewayServices をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2025 年 11 月 12 日 20:34 UTC
- 編集日時: 2025 年 11 月 15 日 19:34 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonECSInfrastructureRoleforExpressGatewayServices

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ServiceLinkedRoleCreateOperations",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "ecs.application-autoscaling.amazonaws.com",
            "elasticloadbalancing.amazonaws.com"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "ELBOperations",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:CreateListener",
        "elasticloadbalancing:CreateLoadBalancer",
        "elasticloadbalancing:CreateRule",
        "elasticloadbalancing:CreateTargetGroup",
        "elasticloadbalancing:ModifyListener",
        "elasticloadbalancing:ModifyRule",
        "elasticloadbalancing:AddListenerCertificates",
        "elasticloadbalancing:RemoveListenerCertificates",
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:DeleteTargetGroup",
        "elasticloadbalancing:DeleteLoadBalancer",
        "elasticloadbalancing:DeleteRule",
        "elasticloadbalancing:DeleteListener"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*",
        "arn:aws:elasticloadbalancing:*:*:listener/app/*/*/*",
        "arn:aws:elasticloadbalancing:*:*:listener-rule/app/*/*/*/*",
        "arn:aws:elasticloadbalancing:*:*:targetgroup/*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "TagOnCreateELBResources",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:AddTags",
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*",
        "arn:aws:elasticloadbalancing:*:*:listener/app/*/*/*",
        "arn:aws:elasticloadbalancing:*:*:listener-rule/app/*/*/*/*",
        "arn:aws:elasticloadbalancing:*:*:targetgroup/*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "elasticloadbalancing:CreateAction" : [
```

```
            "CreateLoadBalancer",
            "CreateListener",
            "CreateRule",
            "CreateTargetGroup"
          ]
        }
      }
    },
    {
      "Sid" : "BlanketAllowCreateSecurityGroupsInVPCs",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSecurityGroup",
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Sid" : "CreateSecurityGroupResourcesWithTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:security-group-rule/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "ModifySecurityGroupOperations",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "TagOnCreateEC2Resources",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:security-group-rule/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateSecurityGroup",
            "AuthorizeSecurityGroupIngress",
            "AuthorizeSecurityGroupEgress"
          ]
        }
      }
    },
    {
      "Sid" : "CertificateOperations",
      "Effect" : "Allow",
      "Action" : [
        "acm:RequestCertificate",
        "acm:AddTagsToCertificate",
        "acm:DeleteCertificate",
        "acm:DescribeCertificate"
      ],
      "Resource" : [
        "arn:aws:acm:*:*:certificate/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
      }
```

```
    },
    {
      "Sid" : "ApplicationAutoscalingCreateOperations",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:RegisterScalableTarget",
        "application-autoscaling:TagResource",
        "application-autoscaling:DeregisterScalableTarget"
      ],
      "Resource" : [
        "arn:aws:application-autoscaling:*:*:scalable-target/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "ApplicationAutoscalingPolicyOperations",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:DeleteScalingPolicy"
      ],
      "Resource" : [
        "arn:aws:application-autoscaling:*:*:scalable-target/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "application-autoscaling:service-namespace" : "ecs"
        }
      }
    },
    {
      "Sid" : "ApplicationAutoscalingReadOperations",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScalingActivities"
      ],
      "Resource" : [
        "arn:aws:application-autoscaling:*:*:scalable-target/*"
```

```
      ]
    },
    {
      "Sid" : "CloudWatchAlarmCreateOperations",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:TagResource"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "CloudWatchAlarmOperations",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "ELBReadOperations",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeRules"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "VPCReadOperations",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchLogsCreateOperations",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:TagResource"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsReadOperations",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonECSInfrastructureRolePolicyForLoadBalancers

説明: ユーザーに代わって ECS ワークロードに関連付けられたロードバランサーを管理するために必要な他の AWS サービスリソースへのアクセスを提供します。

AmazonECSInfrastructureRolePolicyForLoadBalancers は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonECSInfrastructureRolePolicyForLoadBalancers をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 7 月 17 日 16:37 UTC
- 編集日時: 2025 年 7 月 25 日 20:22 UTC
- ARN: arn:aws:iam::aws:policy/AmazonECSInfrastructureRolePolicyForLoadBalancers

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
      "Sid" : "ELBReadOperations",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TargetGroupOperations",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:DeregisterTargets"
      ],
      "Resource" : "arn:aws:elasticloadbalancing:*:*:targetgroup/*/*"
    },
    {
      "Sid" : "ALBModifyListeners",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:ModifyListener",
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:listener/app/*/*/*"
      ]
    },
    {
      "Sid" : "NLBModifyListeners",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:ModifyListener",
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:listener/net/*/*/*"
      ]
    },
    {
      "Sid" : "ALBModifyRules",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:ModifyRule",
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:listener-rule/app/*/*/*/*"
      ]
    }
  ]
```

```
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonECSInfrastructureRolePolicyForManagedInstances

説明: EC2 マネージドリソースを作成および管理するための ECS アクセスを提供します

`AmazonECSInfrastructureRolePolicyForManagedInstances` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonECSInfrastructureRolePolicyForManagedInstances` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 9 月 26 日 18:04 UTC
- 編集日時: 2025 年 12 月 15 日 22:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonECSInfrastructureRolePolicyForManagedInstances`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateLaunchTemplateForManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "CreateLaunchTemplateVersionsForManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ManagedResourceOperator" : "ecs.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ProvisionEC2InstancesForManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateFleet"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:fleet/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "CreateFleetForSupportingResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateFleet"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*::image/*"
      ]
    },
    {
      "Sid" : "RunInstancesForManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "RunInstancesForECSManagedLaunchTemplates",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "RunInstancesForSupportingResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*::image/*"
      ]
    },
    {
      "Sid" : "TagOnCreateEC2ResourcesForManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:fleet/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateFleet",
            "CreateLaunchTemplate",
            "RunInstances"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "PassInstanceRoleForManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/ecsInstanceRole*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CreateServiceLinkedRoleForEC2Spot",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/spot.amazonaws.com/
AWSServiceRoleForEC2Spot"
      ]
    },
    {
      "Sid" : "DescribeEC2ResourcesManagedByECS",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerS

説明: プライベート認証機関、 AWS Secrets Manager、およびユーザーに代わって ECS Service Connect TLS 機能を管理する AWS のサービス ために必要なその他の への管理アクセスを提供します。

AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2024 年 1 月 19 日 20:08 UTC
- 編集日時: 2025 年 11 月 13 日 22:34 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateSecret",
      "Effect" : "Allow",
      "Action" : "secretsmanager:CreateSecret",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:ecs-sc!*",
      "Condition" : {
        "ArnLike" : {
          "aws:RequestTag/AmazonECSCreated" : [
            "arn:aws:ecs:*:*:service/*/*",
            "arn:aws:ecs:*:*:task-set/*/*"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagOnCreateSecret",
      "Effect" : "Allow",
      "Action" : "secretsmanager:TagResource",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:ecs-sc!*",
      "Condition" : {
        "ArnLike" : {
          "aws:RequestTag/AmazonECSCreated" : [
            "arn:aws:ecs:*:*:service/*/*",
            "arn:aws:ecs:*:*:task-set/*/*"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "RotateTLSCertificateSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:UpdateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue",
        "secretsmanager:DeleteSecret",
        "secretsmanager:RotateSecret",
        "secretsmanager:UpdateSecretVersionStage"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:ecs-sc!*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "ecs-sc",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DescribeTLSCertificateSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:ecs-sc!*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ManagePrivateCertificateAuthority",
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:GetCertificate",
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:DescribeCertificateAuthority"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "ManagePrivateCertificateAuthorityForIssuingEndEntityCertificate",
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true",
          "acm-pca:TemplateArn" : "arn:aws:acm-pca:::template/EndEntityCertificate/V1"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonECSInfrastructureRolePolicyForVolumes

説明: ユーザーに代わって ECS ワークロードに関連付けられたボリュームを管理するために必要な他の AWS サービスリソースへのアクセスを提供します。

AmazonECSInfrastructureRolePolicyForVolumes は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonECSInfrastructureRolePolicyForVolumes をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2024 年 1 月 10 日 22:56 UTC
- 編集日時: 2025 年 5 月 28 日 20:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonECSInfrastructureRolePolicyForVolumes`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateEBSManagedVolume",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVolume",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "ArnLike" : {
          "aws:RequestTag/AmazonECSCreated" : "arn:aws:ecs:*:*:task/*"
        },
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "CreateEBSManagedVolumeFromSnapshot",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVolume",
      "Resource" : "arn:aws:ec2:*:*:snapshot/*"
```

```
    },
    {
      "Sid" : "TagOnCreateVolume",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "ArnLike" : {
          "aws:RequestTag/AmazonECSCreated" : "arn:aws:ecs:*:*:task/*"
        },
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVolume",
          "aws:RequestTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "DescribeVolumesForLifecycle",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVolumes",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeInstancesForAttachingVolume",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ManageEBSVolumeLifecycle",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true"
```

```
        }
      }
    },
    {
      "Sid" : "ManageVolumeAttachmentsForEC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Sid" : "DeleteEBSManagedVolume",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteVolume",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "ArnLike" : {
          "aws:ResourceTag/AmazonECSCreated" : "arn:aws:ecs:*:*:task/*"
        },
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonECSInfrastructureRolePolicyForVpcLattice

説明: ユーザーに代わって ECS ワークロードの VPC Lattice 機能を管理するために必要な他の AWS サービスリソースへのアクセスを提供します。

AmazonECSInfrastructureRolePolicyForVpcLattice は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonECSInfrastructureRolePolicyForVpcLattice をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 11 月 15 日 20:02 UTC
- 編集日時: 2024 年 11 月 15 日 20:02 UTC
- ARN: arn:aws:iam::aws:policy/AmazonECSInfrastructureRolePolicyForVpcLattice

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ManagedVpcLatticeTargetRegistration",
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:RegisterTargets",
        "vpc-lattice:DeregisterTargets"
      ],
      "Resource" : [
        "arn:aws:vpc-lattice:*:*:targetgroup/*"
      ]
```

```
    },
    {
      "Sid" : "DescribeVpcLatticeTargetGroup",
      "Effect" : "Allow",
      "Action" : "vpc-lattice:GetTargetGroup",
      "Resource" : [
        "arn:aws:vpc-lattice:*:*:targetgroup/*"
      ]
    },
    {
      "Sid" : "ListVpcLatticeTargets",
      "Effect" : "Allow",
      "Action" : "vpc-lattice:ListTargets",
      "Resource" : [
        "arn:aws:vpc-lattice:*:*:targetgroup/*"
      ]
    },
    {
      "Sid" : "DescribeEc2Resources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeInstances"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonECSInstanceRolePolicyForManagedInstances

説明: Amazon ECS マネージドインスタンスの Amazon ECS インスタンスロールのデフォルトポリシー。

`AmazonECSInstanceRolePolicyForManagedInstances` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonECSInstanceRolePolicyForManagedInstances` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 9 月 26 日 23:49 UTC
- 編集日時: 2025 年 9 月 26 日 23:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonECSInstanceRolePolicyForManagedInstances`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ECSAgentDiscoverPollEndpointPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecs:DiscoverPollEndpoint"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "ECSAgentRegisterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecs:RegisterContainerInstance"
      ],
      "Resource" : "arn:aws:ecs:*:*:cluster/*"
    },
    {
      "Sid" : "ECSAgentPollPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecs:Poll"
      ],
      "Resource" : "arn:aws:ecs:*:*:container-instance/*"
    },
    {
      "Sid" : "ECSAgentTelemetryPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecs:StartTelemetrySession",
        "ecs:PutSystemLogEvents"
      ],
      "Resource" : "arn:aws:ecs:*:*:container-instance/*"
    },
    {
      "Sid" : "ECSAgentStateChangePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecs:SubmitAttachmentStateChanges",
        "ecs:SubmitTaskStateChange"
      ],
      "Resource" : "arn:aws:ecs:*:*:cluster/*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonECSServiceRolePolicy

説明: Amazon ECS がクラスターを管理できるようにするポリシー。

AmazonECSServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 10 月 14 日 01:18 UTC
- 編集日時: 2025 年 11 月 20 日 23:49 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonECSServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v14 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
      "Action" : [
        "ec2:AttachNetworkInterface",
        "ec2:AssociateTrunkInterface",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:Describe*",
        "ec2:DetachNetworkInterface",
        "ec2:DisassociateTrunkInterface",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:Describe*",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:RegisterTargets",
        "route53:ChangeResourceRecordSets",
        "route53:CreateHealthCheck",
        "route53:DeleteHealthCheck",
        "route53:Get*",
        "route53:List*",
        "route53:UpdateHealthCheck",
        "servicediscovery:DeregisterInstance",
        "servicediscovery:Get*",
        "servicediscovery:List*",
        "servicediscovery:RegisterInstance",
        "servicediscovery:UpdateInstanceCustomHealthStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AutoScaling",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AutoScalingManagement",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DeletePolicy",
        "autoscaling:PutScalingPolicy",
        "autoscaling:SetInstanceProtection",
```

```
        "autoscaling:UpdateAutoScalingGroup",
        "autoscaling:PutLifecycleHook",
        "autoscaling:DeleteLifecycleHook",
        "autoscaling:CompleteLifecycleAction",
        "autoscaling:RecordLifecycleActionHeartbeat"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "autoscaling:ResourceTag/AmazonECSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "AutoScalingPlanManagement",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling-plans:CreateScalingPlan",
        "autoscaling-plans:DeleteScalingPlan",
        "autoscaling-plans:DescribeScalingPlans",
        "autoscaling-plans:DescribeScalingPlanResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EventBridge",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/ecs-managed-*"
    },
    {
      "Sid" : "EventBridgeRuleManagement",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "ecs.amazonaws.com"
```

```
        }
      }
    },
    {
      "Sid" : "CWAlarmManagement",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:*"
    },
    {
      "Sid" : "ECSTagging",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*"
    },
    {
      "Sid" : "CWLogGroupManagement",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/ecs/*"
    },
    {
      "Sid" : "CWLogStreamManagement",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/ecs/*:log-stream:*"
    },
    {
      "Sid" : "ExecuteCommandSessionManagement",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ssm:DescribeSessions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ExecuteCommand",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:task/*",
        "arn:aws:ssm:*:*:document/AmazonECS-ExecuteInteractiveCommand"
      ]
    },
    {
      "Sid" : "CloudMapResourceCreation",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:CreateHttpNamespace",
        "servicediscovery:CreateService"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonECSManaged"
          ]
        }
      }
    },
    {
      "Sid" : "CloudMapResourceTagging",
      "Effect" : "Allow",
      "Action" : "servicediscovery:TagResource",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AmazonECSManaged" : "*"
        }
      }
    },
    {
```

```
      "Sid" : "CloudMapResourceDeletion",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DeleteService"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonECSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "CloudMapResourceDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DiscoverInstances",
        "servicediscovery:DiscoverInstancesRevision"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudMapResourceAttributeManagement",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:UpdateServiceAttributes"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonECSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ReadOnlyPermissionsForInstanceEventWindows",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceEventWindows"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonECSTaskExecutionRolePolicy

説明: Amazon ECS タスクの実行に必要な他の AWS サービスリソースへのアクセスを提供します

`AmazonECSTaskExecutionRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonECSTaskExecutionRolePolicy` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2017 年 11 月 16 日 18:48 UTC
- 編集日時: 2017 年 11 月 16 日 18:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonECSTaskExecutionRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonEFSCSIDriverPolicy

説明: EFS リソースへの管理アクセスと EC2 への読み取りアクセスを提供します

AmazonEFSCSIDriverPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEFSCSIDriverPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 7 月 25 日 20:10 UTC

- 編集日時: 2023 年 7 月 25 日 20:10 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEFSCSIDriverPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonEKS_CNI_Policy

説明: このポリシーは、EKS ワーカーノードの IP アドレス設定を変更するために必要なアクセス許可を Amazon VPC CNI プラグイン (amazon-vpc-cni-k8s) に提供します。このアクセス許可セットにより、CNI はユーザーに代わって Elastic Network Interface の一覧表示、説明、変更を行うことができます。 AWS VPC CNI プラグインの詳細については、https://github.com/aws/amazon-vpc-cni-k8s を参照してください。

AmazonEKS_CNI_Policy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEKS_CNI_Policy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 5 月 27 日 21:07 UTC
- 編集日時: 2024 年 3 月 4 日 20:20 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEKS_CNI_Policy

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonEKSBlockStoragePolicy

説明: クラスターのブロックストレージリソースを管理するアクセス許可を付与する EKS クラスターロールにアタッチされたポリシー。

AmazonEKSBlockStoragePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEKSBlockStoragePolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 10 月 30 日 20:18 UTC
- 編集日時: 2024 年 10 月 30 日 20:18 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEKSBlockStoragePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:DetachVolume",
        "ec2:ModifyVolume",
        "ec2:EnableFastSnapshotRestores"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateVolume",
            "CreateSnapshot"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "eks:eks-cluster-name",
            "CSIVolumeName",
            "ebs.csi.eks.amazonaws.com/cluster",
            "kubernetes.io/cluster/*",
            "kubernetes.io/created-for/*",
            "Name",
            "KubernetesCluster"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "eks:eks-cluster-name",
            "CSIVolumeSnapshotName",
            "ebs.csi.eks.amazonaws.com/cluster",
            "kubernetes.io/cluster/*",
            "Name"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonEKSClusterPolicy

説明: このポリシーは、ユーザーに代わってリソースを管理するために必要なアクセス許可を Kubernetes に提供します。Kubernetes では、インスタンス、セキュリティグループ、Elastic Network Interface を含むがこれらに限定されない EC2 リソースに識別情報を配置するには、Ec2:CreateTags 権限が必要です。

AmazonEKSClusterPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEKSClusterPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 5 月 27 日 21:06 UTC
- 編集日時: 2025 年 4 月 17 日 02:52 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEKSClusterPolicy

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonEKSClusterPolicy",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:UpdateAutoScalingGroup",
        "ec2:AttachVolume",
```

```
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateRoute",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:DeleteRoute",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteVolume",
        "ec2:DescribeInstances",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:DetachVolume",
        "ec2:ModifyInstanceAttribute",
        "ec2:ModifyVolume",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeInstanceTopology",
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
        "elasticloadbalancing:AttachLoadBalancerToSubnets",
        "elasticloadbalancing:ConfigureHealthCheck",
        "elasticloadbalancing:CreateListener",
        "elasticloadbalancing:CreateLoadBalancer",
        "elasticloadbalancing:CreateLoadBalancerListeners",
        "elasticloadbalancing:CreateLoadBalancerPolicy",
        "elasticloadbalancing:CreateTargetGroup",
        "elasticloadbalancing:DeleteListener",
        "elasticloadbalancing:DeleteLoadBalancer",
        "elasticloadbalancing:DeleteLoadBalancerListeners",
        "elasticloadbalancing:DeleteTargetGroup",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancerPolicies",
```

```
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DetachLoadBalancerFromSubnets",
        "elasticloadbalancing:ModifyListener",
        "elasticloadbalancing:ModifyLoadBalancerAttributes",
        "elasticloadbalancing:ModifyTargetGroup",
        "elasticloadbalancing:ModifyTargetGroupAttributes",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:SetLoadBalancerPoliciesForBackendServer",
        "elasticloadbalancing:SetLoadBalancerPoliciesOfListener",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonEKSClusterPolicySLRCreate",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonEKSClusterPolicyENIDelete",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteNetworkInterface",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/eks:eni:owner" : "amazon-vpc-cni"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonEKSComputePolicy

説明: クラスターのコンピューティングリソースを管理するアクセス許可を付与する EKS クラスターロールにアタッチされたポリシー。

AmazonEKSComputePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEKSComputePolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 11 月 1 日 21:46 UTC
- 編集日時: 2025 年 6 月 20 日 21:07 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEKSComputePolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateFleet",
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:capacity-reservation/*",
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateFleet",
        "ec2:RunInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateFleet",
        "ec2:RunInstances",
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        },
        "StringLike" : {
          "aws:RequestTag/eks:kubernetes-node-class-name" : "*",
          "aws:RequestTag/eks:kubernetes-node-pool-name" : "*"
```

```
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "eks:eks-cluster-name",
            "eks:kubernetes-node-class-name",
            "eks:kubernetes-node-pool-name",
            "kubernetes.io/cluster/*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateFleet",
            "RunInstances",
            "CreateLaunchTemplate"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:AddRoleToInstanceProfile",
      "Resource" : "arn:aws:iam::*:instance-profile/eks*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/spot.amazonaws.com/
AWSServiceRoleForEC2Spot"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "spot.amazonaws.com"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonEKSConnectorServiceRolePolicy

説明: このポリシーにより、Amazon EKS は EKS コネクタの AWS リソースを管理できます。

AmazonEKSConnectorServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 9 月 4 日 20:31 UTC

- 編集日時: 2025 年 10 月 15 日 22:34 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonEKSConnectorServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AccessSSMService",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateActivation",
        "ssm:DescribeInstanceInformation",
        "ssm:DeleteActivation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConnectorAgentStartSession",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
        "arn:aws:eks:*:*:cluster/*",
        "arn:aws:ssm:*::document/AmazonEKS-ExecuteNonInteractiveCommand"
      ]
    },
    {
      "Sid" : "ConnectorAgentDeregister",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ssm:DeregisterManagedInstance"
      ],
      "Resource" : [
        "arn:aws:eks:*:*:cluster/*"
      ]
    },
    {
      "Sid" : "PassAnyRoleToSsm",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PutManagedEventRule",
      "Effect" : "Allow",
      "Action" : "events:PutRule",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "eks-connector.amazonaws.com"
        },
        "ForAllValues:StringEquals" : {
          "events:source" : "aws.ssm"
        }
      }
    },
    {
      "Sid" : "PutManagedEventTarget",
      "Effect" : "Allow",
      "Action" : "events:PutTargets",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "eks-connector.amazonaws.com"
```

```
        }
      }
    },
    {
      "Sid" : "OpenDataChannel",
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "arn:aws:ssm:*:*:session/*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonEKSDashboardConsoleReadOnly

説明: Amazon EKS コンソールでダッシュボードを表示するための読み取り専用アクセスを提供します。ダッシュボードは、 AWS Organizations を使用して、複数のクラスターおよび関連リソースに関する情報を集約します。

`AmazonEKSDashboardConsoleReadOnly` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonEKSDashboardConsoleReadOnly` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 6 月 19 日 17:22 UTC
- 編集日時: 2025 年 6 月 19 日 17:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSDashboardConsoleReadOnly`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonEKSDashboardReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "eks:ListDashboardData",
        "eks:ListDashboardResources",
        "eks:DescribeClusterVersions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonOrganizationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListRoots",
        "organizations:ListAccountsForParent",
        "organizations:ListOrganizationalUnitsForParent"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonOrganizationsDelegatedAdmin",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : [
        "*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "eks.amazonaws.com"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonEKSDashboardServiceRolePolicy

説明: このポリシーにより、Amazon EKS ダッシュボードは組織全体の情報にアクセスして表示できます。このポリシーにより、EKS Dashboard サービスは AWS Organizations の構造とアカウントに関する情報を収集できます。

`AmazonEKSDashboardServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2025 年 5 月 8 日 19:07 UTC
- 編集日時: 2025 年 5 月 8 日 19:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSDashboardServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowOrganizationsReadActions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:ListRoots",
        "organizations:ListChildren",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonEKSFargatePodExecutionRolePolicy

説明: AWS Fargate で Amazon EKS ポッドを実行するために必要な他の AWS サービスリソースへのアクセスを提供します

AmazonEKSFargatePodExecutionRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEKSFargatePodExecutionRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 11 月 22 日 04:34 UTC
- 編集日時: 2019 年 11 月 22 日 04:34 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEKSFargatePodExecutionRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonEKSForFargateServiceRolePolicy

説明: このポリシーは、Fargate タスクを実行するために必要なアクセス権限を Amazon EKS に付与します。

AmazonEKSForFargateServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 11 月 22 日 04:36 UTC
- 編集日時: 2019 年 11 月 22 日 04:36 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonEKSForFargateServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonEKSLoadBalancingPolicy

説明: クラスターの負荷分散リソースを管理するアクセス許可を付与する EKS クラスターロールにアタッチされたポリシー。

AmazonEKSLoadBalancingPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEKSLoadBalancingPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 10 月 30 日 20:18 UTC
- 編集日時: 2025 年 1 月 9 日 22:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSLoadBalancingPolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:CreateLoadBalancer",
        "elasticloadbalancing:CreateTargetGroup",
        "elasticloadbalancing:CreateListener",
        "elasticloadbalancing:CreateRule",
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "eks:eks-cluster-name",
            "ingress.eks.amazonaws.com/stack",
            "ingress.eks.amazonaws.com/resource",
```

```
            "service.eks.amazonaws.com/stack",
            "service.eks.amazonaws.com/resource"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterTargets"
      ],
      "Resource" : "arn:aws:elasticloadbalancing:*:*:targetgroup/*/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group-rule/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress"
```

```
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/Name" : "eks-cluster-sg*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "elasticloadbalancing:CreateAction" : [
            "CreateLoadBalancer",
            "CreateTargetGroup",
            "CreateListener",
            "CreateRule"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateSecurityGroup",
            "AuthorizeSecurityGroupIngress"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:ModifyLoadBalancerAttributes",
        "elasticloadbalancing:SetIpAddressType",
        "elasticloadbalancing:SetSecurityGroups",
        "elasticloadbalancing:SetSubnets",
        "elasticloadbalancing:ModifyTargetGroup",
        "elasticloadbalancing:ModifyTargetGroupAttributes",
        "elasticloadbalancing:ModifyListener",
        "elasticloadbalancing:AddListenerCertificates",
        "elasticloadbalancing:ModifyListenerAttributes",
        "elasticloadbalancing:RemoveListenerCertificates",
        "elasticloadbalancing:ModifyRule"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "wafv2:AssociateWebACL",
        "wafv2:DisassociateWebACL"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:*/webacl/*/*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "shield:CreateProtection"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "eks:eks-cluster-name",
            "ingress.eks.amazonaws.com/stack",
            "ingress.eks.amazonaws.com/resource",
            "service.eks.amazonaws.com/stack",
            "service.eks.amazonaws.com/resource"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "shield:DeleteProtection"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "shield:TagResource"
      ],
      "Resource" : "arn:aws:shield::*:protection/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "eks:eks-cluster-name",
            "ingress.eks.amazonaws.com/stack",
            "ingress.eks.amazonaws.com/resource",
            "service.eks.amazonaws.com/stack",
            "service.eks.amazonaws.com/resource"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:DescribeUserPoolClient",
        "acm:ListCertificates",
        "acm:DescribeCertificate",
        "wafv2:GetWebACL",
        "wafv2:GetWebACLForResource",
        "elasticloadbalancing:SetWebAcl",
        "elasticloadbalancing:DescribeTargetGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeRouteTables",
        "ec2:DescribeCoipPools",
        "ec2:GetCoipPoolUsage",
        "ec2:GetSecurityGroupsForVpc",
```

```
        "ec2:DescribeVpcPeeringConnections"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
elasticloadbalancing.amazonaws.com/AWSServiceRoleForElasticLoadBalancing",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonEKSLocalOutpostClusterPolicy

説明: このポリシーは、アカウントで実行されている EKS ローカルクラスターのコントロールプレーンインスタンスに対して、ユーザーに代わってリソースを管理するアクセス許可を付与します。

AmazonEKSLocalOutpostClusterPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEKSLocalOutpostClusterPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 8 月 24 日 21:56 UTC
- 編集日時: 2024 年 10 月 24 日 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSLocalOutpostClusterPolicy`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeRouteTables",
        "ec2:DescribeTags",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeAvailabilityZones",
        "ec2messages:AcknowledgeMessage",
        "ec2messages:DeleteMessage",
        "ec2messages:FailMessage",
        "ec2messages:GetEndpoint",
        "ec2messages:GetMessages",
        "ec2messages:SendReply",
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel",
        "ssm:DescribeInstanceProperties",
```

```
        "ssm:DescribeDocumentParameters",
        "ssm:ListInstanceAssociations",
        "ssm:RegisterManagedInstance",
        "ssm:UpdateInstanceInformation",
        "ssm:UpdateInstanceAssociationStatus",
        "ssm:PutComplianceItems",
        "ssm:PutInventory",
        "ecr-public:GetAuthorizationToken",
        "ecr:GetAuthorizationToken"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/eks/*",
        "arn:aws:ecr:*:*:repository/bottlerocket-admin",
        "arn:aws:ecr:*:*:repository/bottlerocket-control-eks",
        "arn:aws:ecr:*:*:repository/diagnostics-collector-eks",
        "arn:aws:ecr:*:*:repository/kubelet-config-updater"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DeleteSecret"
      ],
      "Resource" : "arn:*:secretsmanager:*:*:secret:eks-local.cluster.x-k8s.io/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/eks/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/eks/*:*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonEKSLocalOutpostServiceRolePolicy

説明: Amazon EKS Local がユーザーに代わって AWS サービスを呼び出すことを許可します。

`AmazonEKSLocalOutpostServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 8 月 23 日 21:53 UTC
- 編集日時: 2025 年 6 月 26 日 18:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSLocalOutpostServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeRouteTables",
        "ec2:DescribeAddresses",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribePlacementGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/eks-local:controlplane-name" : "*"
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/eks-local:controlplane-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/eks-local:controlplane-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/eks-local:controlplane-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:placement-group/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:TerminateInstances",
        "ec2:GetConsoleOutput"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/eks-local:controlplane-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "kubernetes.io/cluster/*",
            "eks*"
          ]
        },
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateNetworkInterface",
            "CreateSecurityGroup",
            "RunInstances"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:eks-local.cluster.x-k8s.io/*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "kubernetes.io/cluster/*",
            "eks*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:eks-local.cluster.x-k8s.io/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/eks-local:controlplane-name" : "*"
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "secretsmanager:DeleteSecret",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:eks-local.cluster.x-k8s.io/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/eks-local:controlplane-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "secretsmanager:DescribeSecret",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:eks-local.cluster.x-k8s.io/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile"
      ],
      "Resource" : "arn:aws:iam::*:instance-profile/eks-local-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
```

```
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ssm:resourceTag/eks-local:controlplane-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : "arn:aws:ssm:*::document/AmazonEKS-ControlPlaneInstanceProxy"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "arn:aws:ssm:*:*:session/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:ResumeSession",
        "ssm:TerminateSession"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "outposts:GetOutpost"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonEKSMCPReadOnlyAccess

説明: Amazon EKS MCP サービスへの読み取り専用アクセスを提供します。このポリシーは、オブザーバビリティ、トラブルシューティング、EKS リソース情報の取得、EKS 最適化提案の取得を目的とした EKS MCP サービスで読み取り専用ツールのみを使用するアクセス許可を付与します。

AmazonEKSMCPReadOnlyAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEKSMCPReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 11 月 20 日 17:19 UTC
- 編集日時: 2025 年 11 月 20 日 17:19 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEKSMCPReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "eks:DescribeCluster",
        "eks:ListClusters",
        "eks:DescribeNodegroup",
        "eks:ListNodegroups",
        "eks:DescribeAddon",
```

```
        "eks:ListAddons",
        "eks:DescribeAccessEntry",
        "eks:ListAccessEntries",
        "eks:DescribeInsight",
        "eks:ListInsights",
        "eks:AccessKubernetesApi"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies",
        "iam:GetRolePolicy",
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sts:GetCallerIdentity"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:StartQuery",
        "logs:GetQueryResults"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "eks-mcp:InvokeMcp",
        "eks-mcp:CallReadOnlyTool"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonEKSNetworkingPolicy

説明: クラスターのネットワークリソースを管理するアクセス許可を付与する EKS クラスターロールにアタッチされたポリシー。

AmazonEKSNetworkingPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEKSNetworkingPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2024 年 10 月 28 日 22:34 UTC
- 編集日時: 2024 年 10 月 28 日 22:34 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEKSNetworkingPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        },
        "StringLike" : {
          "aws:RequestTag/eks:kubernetes-cni-node-name" : "*"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "eks:eks-cluster-name",
            "eks:kubernetes-cni-node-name"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachNetworkInterface",
        "ec2:DetachNetworkInterface",
        "ec2:UnassignPrivateIpAddresses",
        "ec2:UnassignIpv6Addresses",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssignIpv6Addresses"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonEKSServicePolicy

説明: このポリシーにより、Amazon Elastic Container Service for Kubernetes が EKS クラスターを操作するために必要なリソースを作成および管理できるようになります。

AmazonEKSServicePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEKSServicePolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 5 月 27 日 21:08 UTC
- 編集日時: 2024 年 10 月 14 日 21:12 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEKSServicePolicy

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DetachNetworkInterface",
```

```
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:ModifyNetworkInterfaceAttribute",
        "iam:ListAttachedRolePolicies",
        "eks:UpdateClusterVersion",
        "ec2:GetSecurityGroupsForVpc"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/Name" : "eks-cluster-*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "route53:AssociateVPCWithHostedZone",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:CreateLogGroup",
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/eks/*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:PutLogEvents",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/eks/*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/eks.amazonaws.com/
AWSServiceRoleForAmazonEKS",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "eks.amazonaws.com"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonEKSServiceRolePolicy

説明: Amazon EKS がユーザーに代わって サービスを呼び出すために必要な AWS サービスにリンクされたロール。

AmazonEKSServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 2 月 21 日 20:10 UTC
- 編集日時: 2025 年 10 月 22 日 23:49 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonEKSServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v10 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DetachNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:CreateSecurityGroup",
        "ec2:CreateNetworkInterfacePermission"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeCoipPools",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSpotPriceHistory",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeRouteTables",
        "ec2:DescribeNetworkAcls",
        "ec2:GetCoipPoolUsage",
        "ec2:GetSecurityGroupsForVpc",
        "eks:DescribeCluster",
        "elasticloadbalancing:DescribeListenerAttributes",
        "elasticloadbalancing:DescribeListenerCertificates",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeSSLPolicies",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeTrustStores",
        "iam:ListAttachedRolePolicies",
        "pricing:GetProducts",
        "shield:GetSubscriptionState",
        "tag:GetResources"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupEgress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/Name" : "eks-cluster-sg*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "kubernetes.io/cluster/*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
```

```
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/Name" : "eks-cluster-*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "route53:AssociateVPCWithHostedZone",
      "Resource" : "arn:aws:route53:::hostedzone/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:CreateLogGroup",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/eks/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/eks/*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:PutLogEvents",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/eks/*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "cloudwatch:namespace" : "AWS/EKS"
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "eks:CreateAccessEntry",
        "eks:DeleteAccessEntry"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "eks:accessEntryType" : "STANDARD"
        },
        "ArnLike" : {
          "eks:principalArn" : "arn:aws:iam::*:role/aws-service-role/eks.amazonaws.com/
AWSServiceRoleForAmazonEKS"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "eks:ListAssociatedAccessPolicies"
      ],
      "Resource" : "arn:aws:eks:*:*:access-entry/*/role/${aws:PrincipalAccount}/
AWSServiceRoleForAmazonEKS/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "eks:AssociateAccessPolicy",
        "eks:DisassociateAccessPolicy"
      ],
      "Resource" : "arn:aws:eks:*:*:access-entry/*/role/${aws:PrincipalAccount}/
AWSServiceRoleForAmazonEKS/*",
      "Condition" : {
        "StringEquals" : {
          "eks:policyArn" : [
            "arn:aws:eks::aws:cluster-access-policy/AmazonEKSComputePolicy",
            "arn:aws:eks::aws:cluster-access-policy/AmazonEKSComputeClusterPolicy",
            "arn:aws:eks::aws:cluster-access-policy/AmazonEKSNetworkingPolicy",
            "arn:aws:eks::aws:cluster-access-policy/AmazonEKSNetworkingClusterPolicy",
            "arn:aws:eks::aws:cluster-access-policy/AmazonEKSLoadBalancingPolicy",
            "arn:aws:eks::aws:cluster-access-policy/
AmazonEKSLoadBalancingClusterPolicy",
            "arn:aws:eks::aws:cluster-access-policy/AmazonEKSBlockStoragePolicy",
```

```
            "arn:aws:eks::aws:cluster-access-policy/
AmazonEKSBlockStorageClusterPolicy",
            "arn:aws:eks::aws:cluster-access-policy/AmazonEKSHybridPolicy",
            "arn:aws:eks::aws:cluster-access-policy/AmazonEKSEventPolicy"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "eks:DescribeAccessEntry",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "eks:accessEntryType" : "EC2"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "events:PutRule",
      "Resource" : "arn:aws:events:*:*:rule/EKS*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "events:source" : [
            "aws.ec2",
            "aws.health"
          ]
        },
        "StringEquals" : {
          "events:ManagedBy" : [
            "eks.amazonaws.com"
```

```
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "events:PutTargets",
      "Resource" : "arn:aws:events:*:*:rule/EKS*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile",
        "iam:CreateInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile"
      ],
      "Resource" : "arn:aws:iam::*:instance-profile/eks*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteLaunchTemplate",
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteLaunchTemplate",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "ec2:ManagedResourceOperator" : [
            "eks.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DeleteListener",
        "elasticloadbalancing:DeleteRule",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:DeleteLoadBalancer",
        "elasticloadbalancing:DeleteTargetGroup",
        "ec2:DeleteSecurityGroup",
        "shield:DescribeProtection"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
```

```
          "aws:ResourceTag/eks:eks-cluster-name" : "*"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonEKSVPCResourceController

説明: VPC リソースコントローラーがワーカーノードの ENI と IP を管理するために使用するポリシーです。

AmazonEKSVPCResourceController は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEKSVPCResourceController をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 8 月 12 日 00:55 UTC
- 編集日時: 2020 年 8 月 12 日 00:55 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEKSVPCResourceController

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonEKSWorkerNodeMinimalPolicy

説明: このポリシーにより、Amazon EKS ワーカーノードは Amazon EKS クラスターに接続できます。

AmazonEKSWorkerNodeMinimalPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEKSWorkerNodeMinimalPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 10 月 02 日 20:03 UTC
- 編集日時: 2024 年 10 月 02 日 20:03 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEKSWorkerNodeMinimalPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "WorkerNodePermissions",
      "Effect" : "Allow",
      "Action" : [
        "eks-auth:AssumeRoleForPodIdentity"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonEKSWorkerNodePolicy

説明: このポリシーにより、Amazon EKS ワーカーノードは Amazon EKS クラスターに接続できます。

AmazonEKSWorkerNodePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEKSWorkerNodePolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 5 月 27 日 21:09 UTC
- 編集日時: 2023 年 11 月 27 日 00:06 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEKSWorkerNodePolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonElastiCacheFullAccess

説明: AWS マネジメントコンソールを介して Amazon ElastiCache へのフルアクセスを提供します。

`AmazonElastiCacheFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonElastiCacheFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2023 年 11 月 28 日 03:49 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElastiCacheFullAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonElastiCacheReadOnlyAccess

説明: AWS マネジメントコンソールを介して Amazon ElastiCache への読み取り専用アクセスを提供します。

AmazonElastiCacheReadOnlyAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonElastiCacheReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2015 年 2 月 6 日 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElastiCacheReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonElasticContainerRegistryPublicFullAccess

説明: Amazon ECR Public リソースへの管理アクセスを提供します

`AmazonElasticContainerRegistryPublicFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonElasticContainerRegistryPublicFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 12 月 1 日 17:25 UTC
- 編集日時: 2020 年 12 月 1 日 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticContainerRegistryPublicFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonElasticContainerRegistryPublicPowerUser

説明: Amazon ECR Public リポジトリへのフルアクセスを提供しますが、リポジトリの削除やポリシーの変更は許可されません。

`AmazonElasticContainerRegistryPublicPowerUser` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonElasticContainerRegistryPublicPowerUser` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2020 年 12 月 1 日 16:16 UTC
- 編集日時: 2020 年 12 月 1 日 16:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticContainerRegistryPublicPowerUser`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonElasticContainerRegistryPublicReadOnly

説明: Amazon ECR パブリックリポジトリへの読み取り専用アクセスを提供します。

`AmazonElasticContainerRegistryPublicReadOnly` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonElasticContainerRegistryPublicReadOnly` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 12 月 1 日 17:27 UTC
- 編集日時: 2020 年 12 月 1 日 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticContainerRegistryPublicReadOnly`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
```

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonElasticFileSystemClientFullAccess

説明: Amazon EFS ファイルシステムへのルートクライアントアクセスを提供します

AmazonElasticFileSystemClientFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonElasticFileSystemClientFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 1 月 13 日 16:27 UTC
- 編集日時: 2020 年 1 月 13 日 16:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemClientFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:ClientMount",
        "elasticfilesystem:ClientRootAccess",
        "elasticfilesystem:ClientWrite",
        "elasticfilesystem:DescribeMountTargets"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonElasticFileSystemClientReadOnlyAccess

説明: Amazon EFS ファイルシステムへの読み取り専用のクライアントアクセスを提供します

AmazonElasticFileSystemClientReadOnlyAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonElasticFileSystemClientReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 1 月 13 日 16:24 UTC
- 編集日時: 2020 年 1 月 13 日 16:24 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticFileSystemClientReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:ClientMount",
        "elasticfilesystem:DescribeMountTargets"
      ],
```

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonElasticFileSystemClientReadWriteAccess

説明: Amazon EFS ファイルシステムへの読み取りと書き込みのクライアントアクセスを提供します

`AmazonElasticFileSystemClientReadWriteAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonElasticFileSystemClientReadWriteAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 1 月 13 日 16:21 UTC
- 編集日時: 2020 年 1 月 13 日 16:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemClientReadWriteAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonElasticFileSystemFullAccess

説明: 経由で Amazon EFS へのフルアクセスを提供します AWS マネジメントコンソール。

`AmazonElasticFileSystemFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonElasticFileSystemFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 5 月 27 日 16:22 UTC

- 編集日時: 2024 年 11 月 7 日 19:34 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticFileSystemFullAccess

ポリシーのバージョン

ポリシーのバージョン: v10 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ElasticFileSystemFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:GetMetricData",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:ModifyNetworkInterfaceAttribute",
        "elasticfilesystem:CreateFileSystem",
        "elasticfilesystem:CreateMountTarget",
        "elasticfilesystem:CreateTags",
        "elasticfilesystem:CreateAccessPoint",
        "elasticfilesystem:CreateReplicationConfiguration",
        "elasticfilesystem:DeleteFileSystem",
        "elasticfilesystem:DeleteMountTarget",
        "elasticfilesystem:DeleteTags",
        "elasticfilesystem:DeleteAccessPoint",
        "elasticfilesystem:DeleteFileSystemPolicy",
```

```
        "elasticfilesystem:DeleteReplicationConfiguration",
        "elasticfilesystem:DescribeAccountPreferences",
        "elasticfilesystem:DescribeBackupPolicy",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeMountTargetSecurityGroups",
        "elasticfilesystem:DescribeTags",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeReplicationConfigurations",
        "elasticfilesystem:ModifyMountTargetSecurityGroups",
        "elasticfilesystem:PutAccountPreferences",
        "elasticfilesystem:PutBackupPolicy",
        "elasticfilesystem:PutLifecycleConfiguration",
        "elasticfilesystem:PutFileSystemPolicy",
        "elasticfilesystem:UpdateFileSystem",
        "elasticfilesystem:UpdateFileSystemProtection",
        "elasticfilesystem:TagResource",
        "elasticfilesystem:UntagResource",
        "elasticfilesystem:ListTagsForResource",
        "elasticfilesystem:Backup",
        "elasticfilesystem:Restore",
        "elasticfilesystem:ReplicationRead",
        "elasticfilesystem:ReplicationWrite",
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateServiceLinkedRoleForEFS",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "elasticfilesystem.amazonaws.com"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "IAMPassRoleAccessForEFS",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "elasticfilesystem.amazonaws.com"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonElasticFileSystemReadOnlyAccess

説明: 経由で Amazon EFS への読み取り専用アクセスを提供します AWS マネジメントコンソール。

`AmazonElasticFileSystemReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonElasticFileSystemReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 5 月 27 日 16:25 UTC
- 編集日時: 2024 年 11 月 7 日 19:39 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v9 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ElasticFileSystemReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:GetMetricData",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "elasticfilesystem:DescribeAccountPreferences",
        "elasticfilesystem:DescribeBackupPolicy",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeMountTargetSecurityGroups",
        "elasticfilesystem:DescribeTags",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeReplicationConfigurations",
        "elasticfilesystem:ListTagsForResource",
        "elasticfilesystem:ReplicationRead",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonElasticFileSystemServiceRolePolicy

説明: Amazon Elastic File System がユーザーに代わって AWS リソースを管理できるようにする

`AmazonElasticFileSystemServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 11 月 5 日 16:52 UTC
- 編集日時: 2024 年 11 月 7 日 19:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonElasticFileSystemServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "backup-storage:MountCapsule",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:ModifyNetworkInterfaceAttribute",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "backup:CreateBackupVault",
        "backup:PutBackupVaultAccessPolicy"
      ],
      "Resource" : [
        "arn:aws:backup:*:*:backup-vault:aws/efs/automatic-backup-vault"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "backup:CreateBackupPlan",
        "backup:CreateBackupSelection"
      ],
      "Resource" : [
```

```
        "arn:aws:backup:*:*:backup-plan:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/backup.amazonaws.com/
AWSServiceRoleForBackup"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "backup.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:CreateReplicationConfiguration",
        "elasticfilesystem:DescribeReplicationConfigurations",
        "elasticfilesystem:DeleteReplicationConfiguration",
        "elasticfilesystem:ReplicationRead",
        "elasticfilesystem:ReplicationWrite"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonElasticFileSystemsUtils

説明: AWS Systems Manager を使用して EC2 インスタンスで Amazon EFS ユーティリティ (amazon-efs-utils) パッケージを自動的に管理し、CloudWatchLog を使用して EFS ファイルシステムのマウントの成功/失敗通知を取得できるようにします。

`AmazonElasticFileSystemsUtils` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonElasticFileSystemsUtils` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 9 月 29 日 15:16 UTC
- 編集日時: 2020 年 9 月 29 日 15:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemsUtils`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
```

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonElasticMapReduceEditorsRole

説明: Amazon Elastic MapReduce Editors サービスロールのデフォルトポリシーです。

AmazonElasticMapReduceEditorsRole は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonElasticMapReduceEditorsRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2018 年 11 月 16 日 21:55 UTC
- 編集日時: 2023 年 2 月 9 日 22:39 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceEditorsRole

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonElasticMapReduceforAutoScalingRole

説明: 自動スケーリング用の Amazon Elastic MapReduce。Auto Scaling が EMR クラスターにインスタンスを追加および削除できるようにするロールです。

AmazonElasticMapReduceforAutoScalingRole は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonElasticMapReduceforAutoScalingRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2016 年 11 月 18 日 01:09 UTC
- 編集日時: 2016 年 11 月 18 日 01:09 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceforAutoScalingRole

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ModifyInstanceGroups"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
```

```
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonElasticMapReduceforEC2Role

説明: Amazon Elastic MapReduce for EC2 サービスロールのデフォルトポリシーです。

`AmazonElasticMapReduceforEC2Role` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonElasticMapReduceforEC2Role` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2017 年 8 月 11 日 23:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceforEC2Role`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonElasticMapReduceFullAccess

説明: このポリシーは非推奨化される予定です。ガイダンスについては、「https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-managed-iam-policies.html」のドキュメントを参照してください。Amazon Elastic MapReduce とそれが必要とする基盤となるサービス (EC2 や S3 など) へのフルアクセスを提供します

`AmazonElasticMapReduceFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonElasticMapReduceFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2019 年 10 月 11 日 15:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticMapReduceFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonElasticMapReducePlacementGroupPolicy

説明: EMR が EC2 プレイスメントグループを作成、記述、削除できるようにするポリシーです。

`AmazonElasticMapReducePlacementGroupPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonElasticMapReducePlacementGroupPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 9 月 29 日 00:37 UTC
- 編集日時: 2020 年 9 月 29 日 00:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticMapReducePlacementGroupPolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonElasticMapReduceReadOnlyAccess

説明: AWS マネジメントコンソール経由で Amazon Elastic MapReduce への読み取り専用アクセスを提供します。

`AmazonElasticMapReduceReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonElasticMapReduceReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2020 年 7 月 29 日 23:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticMapReduceReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonElasticMapReduceRole

説明: このポリシーは非推奨化される予定です。ガイダンスについては、「https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-managed-iam-policies.html」のドキュメントを参照してください。Amazon Elastic MapReduce サービスロールのデフォルトポリシーです。

`AmazonElasticMapReduceRole` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonElasticMapReduceRole` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2020 年 6 月 24 日 22:24 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceRole`

ポリシーのバージョン

ポリシーのバージョン: v10 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
```

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

```
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonElasticsearchServiceRolePolicy

説明: Amazon Elasticsearch Service がユーザーに代わって EC2 Networking APIsなどの他の AWS サービスにアクセスできるようにします。

`AmazonElasticsearchServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 7 月 7 日 00:15 UTC
- 編集日時: 2023 年 10 月 23 日 06:58 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonElasticsearchServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonElasticTranscoder_FullAccess

説明: Elastic Transcoder へのフルアクセスと、Elastic Transcoder の全機能の使用に必要な関連サービスへのアクセスをユーザーに付与します。

AmazonElasticTranscoder_FullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonElasticTranscoder_FullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 4 月 27 日 18:59 UTC
- 編集日時: 2019 年 6 月 10 日 22:51 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticTranscoder_FullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonElasticTranscoder_JobsSubmitter

説明: プリセットの変更、ジョブの送信、Elastic Transcoder 設定の閲覧のためのアクセス許可をユーザーに付与します。このポリシーでは、S3、IAM、SNS など、Elastic Transcode コンソールの使用に必要なその他のサービスへの読み取り専用アクセスも一部付与されます。

`AmazonElasticTranscoder_JobsSubmitter` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonElasticTranscoder_JobsSubmitter` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2018 年 6 月 7 日 21:12 UTC
- 編集日時: 2019 年 6 月 10 日 22:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticTranscoder_JobsSubmitter`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonElasticTranscoder_ReadOnlyAccess

説明: Elastic Transcoder への読み取り専用のアクセスと、関連サービスへのリストアクセスをユーザーに付与します。

AmazonElasticTranscoder_ReadOnlyAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonElasticTranscoder_ReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 6 月 7 日 21:09 UTC
- 編集日時: 2019 年 6 月 10 日 22:48 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticTranscoder_ReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "iam:ListRoles",
        "sns:ListTopics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonElasticTranscoderRole

説明: Amazon Elastic Transcoder サービスロールのデフォルトポリシー。

`AmazonElasticTranscoderRole` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonElasticTranscoderRole` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2019 年 6 月 13 日 22:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticTranscoderRole`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonEMRCleanupPolicy

説明: EMR Service ロールがその機能を失った場合に、EMR が AWS EC2 リソースを終了および削除するために必要なアクションを許可します。

AmazonEMRCleanupPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 9 月 26 日 23:54 UTC
- 編集日時: 2020 年 9 月 29 日 21:11 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonEMRCleanupPolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonEMRContainersServiceRolePolicy

説明: Amazon EMR の実行に必要な他の AWS サービスリソースへのアクセスを許可します

AmazonEMRContainersServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー

- 作成日時: 2020 年 12 月 9 日 00:38 UTC
- 編集日時: 2025 年 2 月 6 日 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEMRContainersServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "eks:DescribeCluster",
        "eks:ListNodeGroups",
        "eks:DescribeNodeGroup",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "eks:ListPodIdentityAssociations",
        "eks:DescribePodIdentityAssociation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:ImportCertificate",
        "acm:AddTagsToCertificate"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/emr-container:endpoint:managed-certificate" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:DeleteCertificate"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/emr-container:endpoint:managed-certificate" : "true"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonEMRFullAccessPolicy_v2

説明: Amazon EMR へのフルアクセスを提供します

AmazonEMRFullAccessPolicy_v2 は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEMRFullAccessPolicy_v2 をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2021 年 3 月 12 日 01:50 UTC
- 編集日時: 2025 年 3 月 27 日 22:07 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEMRFullAccessPolicy_v2

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RunJobFlowExplicitlyWithEMRManagedTag",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:RunJobFlow"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "ElasticMapReduceActions",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:AddInstanceFleet",
        "elasticmapreduce:AddInstanceGroups",
        "elasticmapreduce:AddJobFlowSteps",
        "elasticmapreduce:AddTags",
        "elasticmapreduce:CancelSteps",
        "elasticmapreduce:CreateEditor",
        "elasticmapreduce:CreatePersistentAppUI",
```

```
        "elasticmapreduce:CreateSecurityConfiguration",
        "elasticmapreduce:DeleteEditor",
        "elasticmapreduce:DeleteSecurityConfiguration",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:DescribeEditor",
        "elasticmapreduce:DescribeJobFlows",
        "elasticmapreduce:DescribePersistentAppUI",
        "elasticmapreduce:DescribeSecurityConfiguration",
        "elasticmapreduce:DescribeStep",
        "elasticmapreduce:DescribeReleaseLabel",
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:GetManagedScalingPolicy",
        "elasticmapreduce:GetAutoTerminationPolicy",
        "elasticmapreduce:GetPersistentAppUIPresignedURL",
        "elasticmapreduce:ListBootstrapActions",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListEditors",
        "elasticmapreduce:ListInstanceFleets",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListSecurityConfigurations",
        "elasticmapreduce:ListSteps",
        "elasticmapreduce:ListSupportedInstanceTypes",
        "elasticmapreduce:ModifyCluster",
        "elasticmapreduce:ModifyInstanceFleet",
        "elasticmapreduce:ModifyInstanceGroups",
        "elasticmapreduce:OpenEditorInConsole",
        "elasticmapreduce:PutAutoScalingPolicy",
        "elasticmapreduce:PutBlockPublicAccessConfiguration",
        "elasticmapreduce:PutManagedScalingPolicy",
        "elasticmapreduce:RemoveAutoScalingPolicy",
        "elasticmapreduce:RemoveManagedScalingPolicy",
        "elasticmapreduce:RemoveTags",
        "elasticmapreduce:SetTerminationProtection",
        "elasticmapreduce:StartEditor",
        "elasticmapreduce:StopEditor",
        "elasticmapreduce:TerminateJobFlows",
        "elasticmapreduce:ViewEventsFromAllClustersInConsole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ViewMetricsInEMRConsole",
      "Effect" : "Allow",
```

```
      "Action" : [
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassRoleForElasticMapReduce",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/EMR_DefaultRole_V2",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "elasticmapreduce.amazonaws.com*"
        }
      }
    },
    {
      "Sid" : "PassRoleForEC2",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/EMR_EC2_DefaultRole",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.amazonaws.com*"
        }
      }
    },
    {
      "Sid" : "PassRoleForAutoScaling",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/EMR_AutoScaling_DefaultRole",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "application-autoscaling.amazonaws.com*"
        }
      }
    },
    {
      "Sid" : "ElasticMapReduceServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
elasticmapreduce.amazonaws.com*/AWSServiceRoleForEMRCleanup*",
```

```
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "elasticmapreduce.amazonaws.com",
            "elasticmapreduce.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleUIActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeNatGateways",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "s3:ListAllMyBuckets",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonEMRReadOnlyAccessPolicy_v2

説明: Amazon EMR と関連する CloudWatch メトリックスへの読み取り専用アクセスを提供します。

AmazonEMRReadOnlyAccessPolicy_v2 は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEMRReadOnlyAccessPolicy_v2 をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 3 月 12 日 01:39 UTC
- 編集日時: 2023 年 8 月 2 日 19:15 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEMRReadOnlyAccessPolicy_v2

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonEMRServerlessServiceRolePolicy

説明: Amazon EMRServerless の実行に必要な他の AWS サービスリソースへのアクセスを許可します

AmazonEMRServerlessServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 5 月 20 日 23:15 UTC
- 編集日時: 2024 年 1 月 25 日 18:21 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEMRServerlessServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonEMRServicePolicy_v2

説明: このポリシーは Amazon EMR サービスロールに使用されるものなので、アカウントの他の IAM ユーザーやロールには使用しないでください。このポリシーは、EMR クラスターのオペレーションに必要な EMR および関連サービスに関連するリソースを作成および管理するためのアクセス許可を付与します。

AmazonEMRServicePolicy_v2 は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEMRServicePolicy_v2 をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2021 年 3 月 12 日 01:11 UTC
- 編集日時: 2025 年 3 月 3 日 20:37 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEMRServicePolicy_v2

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateInTaggedNetwork",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:RunInstances",
        "ec2:CreateFleet",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
```

```
    {
      "Sid" : "CreateWithEMRTaggedLaunchTemplate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateFleet",
        "ec2:RunInstances",
        "ec2:CreateLaunchTemplateVersion"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "CreateEMRTaggedLaunchTemplate",
      "Effect" : "Allow",
      "Action" : "ec2:CreateLaunchTemplate",
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "CreateEMRTaggedInstancesAndVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateFleet"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
```

```
      "Sid" : "ResourcesToLaunchEC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateFleet",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*::image/ami-*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:capacity-reservation/*",
        "arn:aws:ec2:*:*:placement-group/EMR_*",
        "arn:aws:ec2:*:*:fleet/*",
        "arn:aws:ec2:*:*:dedicated-host/*",
        "arn:aws:resource-groups:*:*:group/*"
      ]
    },
    {
      "Sid" : "ManageEMRTaggedResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyInstanceAttribute",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "ManageTagsOnEMRTaggedResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "CreateNetworkInterfaceNeededForPrivateSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "TagOnCreateTaggedEMRResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances",
            "CreateFleet",
            "CreateLaunchTemplate",
```

```
            "CreateNetworkInterface"
          ]
        }
      }
    },
    {
      "Sid" : "TagPlacementGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:placement-group/EMR_*"
      ]
    },
    {
      "Sid" : "ListActionsForEC2Resources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumeStatus",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateDefaultSecurityGroupWithEMRTags",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "CreateDefaultSecurityGroupInVPCWithEMRTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "TagOnCreateDefaultSecurityGroupWithEMRTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true",
          "ec2:CreateAction" : "CreateSecurityGroup"
        }
      }
    },
    {
      "Sid" : "ManageSecurityGroups",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "CreateEMRPlacementGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreatePlacementGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:placement-group/EMR_*"
    },
    {
      "Sid" : "DeletePlacementGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeletePlacementGroup"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AutoScaling",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ResourceGroupsForCapacityReservations",
```

```
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:ListGroupResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AutoScalingCloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:*_EMR_Auto_Scaling"
    },
    {
      "Sid" : "PassRoleForAutoScaling",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/EMR_AutoScaling_DefaultRole",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "application-autoscaling.amazonaws.com*"
        }
      }
    },
    {
      "Sid" : "PassRoleForEC2",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/EMR_EC2_DefaultRole",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.amazonaws.com*"
        }
      }
    },
    {
      "Sid" : "CreateAndModifyEmrServiceVPCEndpoint",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint",
        "ec2:CreateVpcEndpoint"
```

```
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "CreateEmrServiceVPCEndpoint",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true",
          "aws:RequestTag/Name" : "emr-service-vpce"
        }
      }
    },
    {
      "Sid" : "TagEmrServiceVPCEndpoint",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint",
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true",
          "aws:RequestTag/Name" : "emr-service-vpce"
        }
      }
    }
```

```
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonESCognitoAccess

説明: Amazon Cognito 設定サービスへの制限付きアクセスを提供します。

AmazonESCognitoAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonESCognitoAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 2 月 28 日 22:29 UTC
- 編集日時: 2021 年 12 月 20 日 14:04 UTC
- ARN: arn:aws:iam::aws:policy/AmazonESCognitoAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する

- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonESFullAccess

説明: Amazon ES 設定サービスへのフルアクセスを提供します。

AmazonESFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonESFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 10 月 1 日 19:14 UTC
- 編集日時: 2015 年 10 月 1 日 19:14 UTC
- ARN: arn:aws:iam::aws:policy/AmazonESFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonESReadOnlyAccess

説明: Amazon ES 設定サービスへの読み取り専用アクセスを提供します。

`AmazonESReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonESReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 10 月 1 日 19:18 UTC
- 編集日時: 2018 年 10 月 3 日 03:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonESReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonEventBridgeApiDestinationsServiceRolePolicy

説明: EventBridge がユーザーに代わって Secret Manager リソースにアクセスすることを許可します。

`AmazonEventBridgeApiDestinationsServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 2 月 11 日 20:52 UTC
- 編集日時: 2025 年 5 月 29 日 21:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEventBridgeApiDestinationsServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:events!connection/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "secretsmanager.*.amazonaws.com",
          "kms:EncryptionContext:SecretARN" : [
            "arn:aws:secretsmanager:*:*:secret:events!connection/*"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/EventBridgeApiDestinations" : "true"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonEventBridgeFullAccess

説明: Amazon EventBridge へのフルアクセス権を提供します。

`AmazonEventBridgeFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonEventBridgeFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 7 月 11 日 14:08 UTC

- 編集日時: 2025 年 1 月 22 日 01:37 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEventBridgeFullAccess

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EventBridgeActions",
      "Effect" : "Allow",
      "Action" : [
        "events:*",
        "schemas:*",
        "scheduler:*",
        "pipes:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMCreateServiceLinkedRoleForApiDestinations",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
apidestinations.events.amazonaws.com/
AWSServiceRoleForAmazonEventBridgeApiDestinations",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "apidestinations.events.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMCreateServiceLinkedRoleForAmazonEventBridgeSchemas",
```

```
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/schemas.amazonaws.com/
AWSServiceRoleForSchemas",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "schemas.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SecretsManagerAccessForApiDestinations",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:events!*"
    },
    {
      "Sid" : "IAMPassRoleAccessForEventBridge",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "events.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMPassRoleAccessForScheduler",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "scheduler.amazonaws.com"
        }
      }
    },
```

```
    {
      "Sid" : "IAMPassRoleAccessForPipes",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "pipes.amazonaws.com"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonEventBridgePipesFullAccess

説明: Amazon EventBridge Pipes へのフルアクセス権を提供します。

`AmazonEventBridgePipesFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonEventBridgePipesFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 12 月 1 日 17:03 UTC
- 編集日時: 2022 年 12 月 1 日 17:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgePipesFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonEventBridgePipesOperatorAccess

説明: Amazon EventBridge Pipes への読み取り専用アクセスとオペレーターアクセス (つまり、Pipes の実行を停止および開始する機能) を提供します。

AmazonEventBridgePipesOperatorAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEventBridgePipesOperatorAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 12 月 1 日 17:04 UTC
- 編集日時: 2022 年 12 月 1 日 17:04 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEventBridgePipesOperatorAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "pipes:DescribePipe",
        "pipes:ListPipes",
        "pipes:ListTagsForResource",
        "pipes:StartPipe",
        "pipes:StopPipe"
```

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonEventBridgePipesReadOnlyAccess

説明: Amazon EventBridge Pipes への読み取り専用アクセスを提供します。

`AmazonEventBridgePipesReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonEventBridgePipesReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 12 月 1 日 17:04 UTC
- 編集日時: 2022 年 12 月 1 日 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgePipesReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonEventBridgeReadOnlyAccess

説明: Amazon EventBridge への読み取り専用アクセスを提供します。

`AmazonEventBridgeReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonEventBridgeReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2019 年 7 月 11 日 13:59 UTC
- 編集日時: 2022 年 12 月 1 日 17:02 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEventBridgeReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonEventBridgeSchedulerFullAccess

説明: AmazonEventBridgeSchedulerFullAccess のマネージドポリシーは、スケジュールおよびスケジュールグループのすべての EventBridge スケジューラアクションを使用する権限を付与します。

`AmazonEventBridgeSchedulerFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEventBridgeSchedulerFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 11 月 10 日 18:37 UTC
- 編集日時: 2025 年 5 月 16 日 19:22 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEventBridgeSchedulerFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonEventBridgeSchedulerReadOnlyAccess

説明: AmazonEventBridgeSchedulerReadOnlyAccess のマネージドポリシーは、スケジュールとスケジュールグループに関する詳細を閲覧する読み取り専用権限を付与します。

`AmazonEventBridgeSchedulerReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonEventBridgeSchedulerReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 11 月 10 日 18:50 UTC
- 編集日時: 2025 年 5 月 16 日 16:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeSchedulerReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "scheduler:ListSchedules",
        "scheduler:ListScheduleGroups",
        "scheduler:GetSchedule",
        "scheduler:GetScheduleGroup",
        "scheduler:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonEventBridgeSchemasFullAccess

説明: Amazon EventBridge スキーマへのフルアクセスを提供します。

`AmazonEventBridgeSchemasFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonEventBridgeSchemasFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 11 月 28 日 23:12 UTC
- 編集日時: 2019 年 11 月 28 日 23:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeSchemasFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonEventBridgeSchemasReadOnlyAccess

説明: Amazon EventBridge スキーマへの読み取り専用アクセスを提供します。

`AmazonEventBridgeSchemasReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonEventBridgeSchemasReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 11 月 28 日 23:05 UTC
- 編集日時: 2020 年 5 月 1 日 00:50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeSchemasReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonEventBridgeSchemasServiceRolePolicy

説明: Amazon EventBridge スキーマによって作成されたマネージドルールへのアクセス許可を付与します。

AmazonEventBridgeSchemasServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 11 月 27 日 01:10 UTC
- 編集日時: 2019 年 11 月 27 日 01:10 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonEventBridgeSchemasServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonEVSServiceRolePolicy

説明: ユーザーに代わってリソースを管理するアクセス許可を EVS に付与します

AmazonEVSServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2025 年 5 月 16 日 23:37 UTC
- 編集日時: 2025 年 8 月 14 日 16:04 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonEVSServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeNetworkStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateEniInSubnetStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "ManageSubnetStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSubnet"
      ],
      "Resource" : "arn:aws:ec2:*:*:subnet/*",
      "Condition" : {
        "Null" : {
```

```
          "aws:ResourceTag/AmazonEVSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "CreateEniWithTagStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AmazonEVSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "TagOnCreateNetworkInterface",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AmazonEVSManaged" : "false"
        },
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateNetworkInterface"
          ]
        }
      }
    },
    {
      "Sid" : "ManageEniStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:AssignIpv6Addresses"
      ],
```

```
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonEVSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ManageInstanceStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:DescribeInstanceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonEVSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DescribeInstanceAndVolumeStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ManageVolumeStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume",
        "ec2:DetachVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonEVSManaged" : "false"
```

```
        }
      }
    },
    {
      "Sid" : "ManageSecretStatement",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DeleteSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonEVSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "UpdateSecurityGroupStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*"
    },
    {
      "Sid" : "CloudWatchPutMetricDataStatement",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/Usage",
            "AWS/EVS"
          ]
        }
      }
    }
  ]
```

```
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonFISServiceRolePolicy

説明: AWS FIS が実験のモニタリングとリソース選択を管理できるようにするポリシー。

AmazonFISServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 12 月 21 日 21:18 UTC
- 編集日時: 2022 年 10 月 25 日 09:05 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonFISServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonForecastFullAccess

説明: Amazon Forecast のすべてのアクションへのアクセス許可

`AmazonForecastFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonForecastFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 1 月 18 日 01:52 UTC

- 編集日時: 2019 年 1 月 18 日 01:52 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonForecastFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "forecast:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "forecast.amazonaws.com"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する

- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonFraudDetectorFullAccessPolicy

説明: Amazon Fraud Detector のすべてのアクションへのアクセスを許可します

AmazonFraudDetectorFullAccessPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonFraudDetectorFullAccessPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 12 月 3 日 22:46 UTC
- 編集日時: 2019 年 12 月 3 日 22:46 UTC
- ARN: arn:aws:iam::aws:policy/AmazonFraudDetectorFullAccessPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonFreeRTOSFullAccess

説明: Amazon FreeRTOS のフルアクセスポリシー

AmazonFreeRTOSFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonFreeRTOSFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 11 月 29 日 15:32 UTC
- 編集日時: 2017 年 11 月 29 日 15:32 UTC
- ARN: arn:aws:iam::aws:policy/AmazonFreeRTOSFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
    {
      "Effect" : "Allow",
      "Action" : [
        "freertos:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonFreeRTOSOTAUpdate

説明: ユーザーに Amazon FreeRTOS OTA Update へのアクセスを許可します

`AmazonFreeRTOSOTAUpdate` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonFreeRTOSOTAUpdate` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2018 年 8 月 27 日 22:43 UTC
- 編集日時: 2020 年 12 月 18 日 17:47 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonFreeRTOSOTAUpdate`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonFSxConsoleFullAccess

説明: 経由で Amazon FSx へのフルアクセスと関連 AWS サービスへのアクセスを提供します AWS マネジメントコンソール。

AmazonFSxConsoleFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonFSxConsoleFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 11 月 28 日 16:36 UTC
- 編集日時: 2025 年 11 月 5 日 20:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFSxConsoleFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v14 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ListResourcesAssociatedWithFSxFileSystem",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "ds:DescribeDirectories",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "firehose:ListDeliveryStreams",
        "kms:ListAliases",
        "logs:DescribeLogGroups",
        "s3:ListBucket",
        "secretsmanager:ListSecrets"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "FullAccessToFSx",
      "Effect" : "Allow",
      "Action" : [
        "fsx:AssociateFileGateway",
        "fsx:AssociateFileSystemAliases",
        "fsx:CancelDataRepositoryTask",
        "fsx:CopyBackup",
        "fsx:CopySnapshotAndUpdateVolume",
        "fsx:CreateAndAttachS3AccessPoint",
        "fsx:CreateBackup",
        "fsx:CreateDataRepositoryAssociation",
        "fsx:CreateDataRepositoryTask",
        "fsx:CreateFileCache",
        "fsx:CreateFileSystem",
        "fsx:CreateFileSystemFromBackup",
        "fsx:CreateSnapshot",
        "fsx:CreateStorageVirtualMachine",
        "fsx:CreateVolume",
        "fsx:CreateVolumeFromBackup",
        "fsx:DeleteBackup",
        "fsx:DeleteDataRepositoryAssociation",
        "fsx:DeleteFileCache",
        "fsx:DeleteFileSystem",
        "fsx:DeleteSnapshot",
        "fsx:DeleteStorageVirtualMachine",
        "fsx:DeleteVolume",
        "fsx:DescribeAssociatedFileGateways",
        "fsx:DescribeBackups",
        "fsx:DescribeDataRepositoryAssociations",
        "fsx:DescribeDataRepositoryTasks",
        "fsx:DescribeFileCaches",
        "fsx:DescribeFileSystemAliases",
        "fsx:DescribeFileSystems",
        "fsx:DescribeS3AccessPointAttachments",
        "fsx:DescribeSharedVpcConfiguration",
        "fsx:DescribeSnapshots",
        "fsx:DescribeStorageVirtualMachines",
        "fsx:DescribeVolumes",
        "fsx:DetachAndDeleteS3AccessPoint",
        "fsx:DisassociateFileGateway",
        "fsx:DisassociateFileSystemAliases",
```

```
        "fsx:ListTagsForResource",
        "fsx:ManageBackupPrincipalAssociations",
        "fsx:ReleaseFileSystemNfsV3Locks",
        "fsx:RestoreVolumeFromSnapshot",
        "fsx:TagResource",
        "fsx:UntagResource",
        "fsx:UpdateDataRepositoryAssociation",
        "fsx:UpdateFileCache",
        "fsx:UpdateFileSystem",
        "fsx:UpdateSharedVpcConfiguration",
        "fsx:UpdateSnapshot",
        "fsx:UpdateStorageVirtualMachine",
        "fsx:UpdateVolume"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateFSxSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "fsx.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreateSLRForLustreS3Integration",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "s3.data-source.lustre.fsx.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreateTags",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:route-table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonFSx" : "ManagedByAmazonFSx"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "fsx.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ManageCrossAccountDataReplication",
      "Effect" : "Allow",
      "Action" : [
        "fsx:PutResourcePolicy",
        "fsx:GetResourcePolicy",
        "fsx:DeleteResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "ram.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonFSxConsoleReadOnlyAccess

説明: Amazon FSx への読み取り専用アクセスと、 を介した関連 AWS サービスへのアクセスを提供します AWS マネジメントコンソール。

AmazonFSxConsoleReadOnlyAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonFSxConsoleReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 11 月 28 日 16:35 UTC
- 編集日時: 2025 年 2 月 25 日 15:07 UTC
- ARN: arn:aws:iam::aws:policy/AmazonFSxConsoleReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
        "cloudwatch:GetMetricData",
        "ds:DescribeDirectories",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "firehose:ListDeliveryStreams",
        "fsx:Describe*",
        "fsx:ListTagsForResource",
        "kms:DescribeKey",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonFSxFullAccess

説明: Amazon FSx へのフルアクセスと関連 AWS サービスへのアクセスを提供します。

AmazonFSxFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonFSxFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 11 月 28 日 16:34 UTC

- 編集日時: 2025 年 6 月 25 日 17:52 UTC
- ARN: arn:aws:iam::aws:policy/AmazonFSxFullAccess

ポリシーのバージョン

ポリシーのバージョン: v11 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ViewAWSDSDirectories",
      "Effect" : "Allow",
      "Action" : [
        "ds:DescribeDirectories"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "FullAccessToFSx",
      "Effect" : "Allow",
      "Action" : [
        "fsx:AssociateFileGateway",
        "fsx:AssociateFileSystemAliases",
        "fsx:CancelDataRepositoryTask",
        "fsx:CopyBackup",
        "fsx:CopySnapshotAndUpdateVolume",
        "fsx:CreateAndAttachS3AccessPoint",
        "fsx:CreateBackup",
        "fsx:CreateDataRepositoryAssociation",
        "fsx:CreateDataRepositoryTask",
        "fsx:CreateFileCache",
        "fsx:CreateFileSystem",
        "fsx:CreateFileSystemFromBackup",
        "fsx:CreateSnapshot",
        "fsx:CreateStorageVirtualMachine",
```

```
        "fsx:CreateVolume",
        "fsx:CreateVolumeFromBackup",
        "fsx:DetachAndDeleteS3AccessPoint",
        "fsx:DeleteBackup",
        "fsx:DeleteDataRepositoryAssociation",
        "fsx:DeleteFileCache",
        "fsx:DeleteFileSystem",
        "fsx:DeleteSnapshot",
        "fsx:DeleteStorageVirtualMachine",
        "fsx:DeleteVolume",
        "fsx:DescribeAssociatedFileGateways",
        "fsx:DescribeBackups",
        "fsx:DescribeDataRepositoryAssociations",
        "fsx:DescribeDataRepositoryTasks",
        "fsx:DescribeFileCaches",
        "fsx:DescribeFileSystemAliases",
        "fsx:DescribeFileSystems",
        "fsx:DescribeS3AccessPointAttachments",
        "fsx:DescribeSharedVpcConfiguration",
        "fsx:DescribeSnapshots",
        "fsx:DescribeStorageVirtualMachines",
        "fsx:DescribeVolumes",
        "fsx:DisassociateFileGateway",
        "fsx:DisassociateFileSystemAliases",
        "fsx:ListTagsForResource",
        "fsx:ManageBackupPrincipalAssociations",
        "fsx:ReleaseFileSystemNfsV3Locks",
        "fsx:RestoreVolumeFromSnapshot",
        "fsx:TagResource",
        "fsx:UntagResource",
        "fsx:UpdateDataRepositoryAssociation",
        "fsx:UpdateFileCache",
        "fsx:UpdateFileSystem",
        "fsx:UpdateSharedVpcConfiguration",
        "fsx:UpdateSnapshot",
        "fsx:UpdateStorageVirtualMachine",
        "fsx:UpdateVolume"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateSLRForFSx",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "fsx.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreateSLRForLustreS3Integration",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "s3.data-source.lustre.fsx.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreateLogsForFSxWindowsAuditLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/fsx/*"
      ]
    },
    {
      "Sid" : "WriteToAmazonKinesisDataFirehose",
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord"
      ],
      "Resource" : [
        "arn:aws:firehose:*:*:deliverystream/aws-fsx-*"
      ]
    },
```

```
    {
      "Sid" : "CreateTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:route-table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonFSx" : "ManagedByAmazonFSx"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "fsx.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DescribeEC2VpcResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSecurityGroups",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "fsx.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ManageCrossAccountDataReplication",
      "Effect" : "Allow",
      "Action" : [
        "fsx:PutResourcePolicy",
```

```
        "fsx:GetResourcePolicy",
        "fsx:DeleteResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "ram.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonFSxReadOnlyAccess

説明: Amazon FSx への読み取り専用アクセスを提供します。

`AmazonFSxReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonFSxReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 11 月 28 日 16:33 UTC
- 編集日時: 2018 年 11 月 28 日 16:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFSxReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonFSxServiceRolePolicy

説明: Amazon FSx がユーザーに代わって AWS リソースを管理することを許可する

AmazonFSxServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 11 月 28 日 10:38 UTC
- 編集日時: 2025 年 7 月 22 日 18:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonFSxServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateFileSystem",
      "Effect" : "Allow",
      "Action" : [
        "ds:AuthorizeApplication",
        "ds:GetAuthorizedApplicationDetails",
        "ds:UnauthorizeApplication",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeAddresses",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
```

```
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DisassociateAddress",
        "ec2:GetSecurityGroupsForVpc",
        "route53:AssociateVPCWithHostedZone"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PutMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/FSx"
        }
      }
    },
    {
      "Sid" : "TagResourceNetworkInterface",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "AmazonFSx.FileSystemId"
        }
      }
    },
    {
      "Sid" : "ManageNetworkInterface",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignIpv6Addresses",
        "ec2:AssignPrivateIpAddresses",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:UnassignIpv6Addresses",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonFSx.FileSystemId" : "false"
        }
      }
    },
    {
      "Sid" : "ManageRouteTable",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateRoute",
        "ec2:ReplaceRoute",
        "ec2:DeleteRoute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:route-table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonFSx" : "ManagedByAmazonFSx"
        }
      }
    },
    {
      "Sid" : "PutCloudWatchLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/fsx/*"
    },
```

```
    {
      "Sid" : "ManageAuditLogs",
      "Effect" : "Allow",
      "Action" : [
        "firehose:DescribeDeliveryStream",
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : "arn:aws:firehose:*:*:deliverystream/aws-fsx-*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonGlacierFullAccess

説明: 経由で Amazon Glacier へのフルアクセスを提供します AWS マネジメントコンソール。

`AmazonGlacierFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonGlacierFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2015 年 2 月 6 日 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGlacierFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonGlacierReadOnlyAccess

説明: 経由で Amazon Glacier への読み取り専用アクセスを提供します AWS マネジメントコンソール。

`AmazonGlacierReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonGlacierReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC

- 編集日時: 2016 年 5 月 5 日 18:46 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGlacierReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する

- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonGrafanaAthenaAccess

説明: このポリシーにより、Amazon Grafana 内の Amazon Athena プラグインからクエリを実行して s3 へのクエリと書き込みの結果を有効にするために必要な、Amazon Athena と依存関係へのアクセス権が付与されます。

`AmazonGrafanaAthenaAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonGrafanaAthenaAccess` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2021 年 11 月 22 日 17:11 UTC
- 編集日時: 2021 年 11 月 22 日 17:11 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonGrafanaAthenaAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonGrafanaCloudWatchAccess

説明: このポリシーにより、CloudWatch を Amazon Managed Grafana 内のデータソースとして使用するために必要な、Amazon CloudWatch とその依存関係へのアクセス権が付与されます。

`AmazonGrafanaCloudWatchAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonGrafanaCloudWatchAccess` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 3 月 24 日 22:41 UTC
- 編集日時: 2023 年 3 月 24 日 22:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonGrafanaCloudWatchAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonGrafanaRedshiftAccess

説明: このポリシーにより、Amazon Grafana で Amazon Redshift プラグインを使用するために必要な、Amazon Redshift およびその依存関係へのスコープ付きアクセスを許可します。

AmazonGrafanaRedshiftAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonGrafanaRedshiftAccess をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2021 年 11 月 26 日 23:15 UTC
- 編集日時: 2021 年 11 月 26 日 23:15 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonGrafanaRedshiftAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonGrafanaServiceLinkedRolePolicy

説明: Amazon Grafana が管理または使用する AWS リソースへのアクセスを提供します。

AmazonGrafanaServiceLinkedRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 11 月 8 日 23:10 UTC
- 編集日時: 2022 年 11 月 8 日 23:10 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonGrafanaServiceLinkedRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonGuardDutyFullAccess

説明: Amazon GuardDuty を使用するためのフルアクセスを提供します。

`AmazonGuardDutyFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonGuardDutyFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 11 月 28 日 22:31 UTC
- 編集日時: 2025 年 11 月 20 日 02:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGuardDutyFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
    {
      "Sid" : "AmazonGuardDutyFullAccessSid1",
      "Effect" : "Allow",
      "Action" : "guardduty:*",
      "Resource" : "*"
    },
    {
      "Sid" : "CreateServiceLinkedRoleSid1",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : [
            "guardduty.amazonaws.com",
            "malware-protection.guardduty.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ActionsForOrganizationsSid1",
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IamGetRoleSid1",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/
*AWSServiceRoleForAmazonGuardDutyMalwareProtection"
    },
    {
      "Sid" : "AllowPassRoleToMalwareProtection",
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "malware-protection-plan.guardduty.amazonaws.com",
            "malware-protection.guardduty.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonGuardDutyFullAccess_v2

説明: Amazon GuardDuty を使用するためのフルアクセスを提供します

`AmazonGuardDutyFullAccess_v2` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonGuardDutyFullAccess_v2` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 6 月 4 日 20:22 UTC
- 編集日時: 2025 年 11 月 20 日 02:19 UTC

- ARN: arn:aws:iam::aws:policy/AmazonGuardDutyFullAccess_v2

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GuardDutyFullAccess",
      "Effect" : "Allow",
      "Action" : "guardduty:*",
      "Resource" : "*"
    },
    {
      "Sid" : "CreateGuardDutyServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "guardduty.amazonaws.com",
            "malware-protection.guardduty.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "GuardDutyOrganizationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
```

```
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GuardDutyOrganizationsAdminAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:DisableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "guardduty.amazonaws.com",
            "malware-protection.guardduty.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "GuardDutyIamRoleAccess",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/
*AWSServiceRoleForAmazonGuardDutyMalwareProtection"
    },
    {
      "Sid" : "AllowPassRoleToMalwareProtection",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "malware-protection-plan.guardduty.amazonaws.com",
            "malware-protection.guardduty.amazonaws.com"
```

```
            ]
          }
        }
      }
    ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonGuardDutyMalwareProtectionServiceRolePolicy

説明: GuardDuty マルウェア保護は、AWSServiceRoleForAmazonGuardDutyMalwareProtection というサービスリンクロール (SLR) を使用します。この サービスリンクロールにより、GuardDuty マルウェア保護はエージェントレススキャンを実行してマルウェアを検出できます。これにより、GuardDuty はアカウントにスナップショットを作成し、そのスナップショットを GuardDuty サービスアカウントと共有し、マルウェアをスキャンできます。共有したこれらのスナップショットを評価し、取得された EC2 インスタンスのメタデータが GuardDuty Malware Protection の検出結果に含まれます。AWSServiceRoleForAmazonGuardDutyMalwareProtection サービスリンクロールは、ロールを継承するために malware-protection.guardduty.amazonaws.com サービスを信頼します。

`AmazonGuardDutyMalwareProtectionServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー

- 作成日時: 2022 年 7 月 19 日 19:06 UTC
- 編集日時: 2024 年 1 月 25 日 22:24 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonGuardDutyMalwareProtectionServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonGuardDutyReadOnlyAccess

説明: Amazon GuardDuty リソースへの読み取り専用アクセスを提供します

AmazonGuardDutyReadOnlyAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonGuardDutyReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 11 月 28 日 22:29 UTC
- 編集日時: 2023 年 11 月 16 日 23:07 UTC
- ARN: arn:aws:iam::aws:policy/AmazonGuardDutyReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonGuardDutyServiceRolePolicy

説明: Amazon Guard Duty が使用または管理する AWS リソースへのアクセスを有効にする

`AmazonGuardDutyServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 11 月 28 日 20:12 UTC
- 編集日時: 2024 年 8 月 12 日 20:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonGuardDutyServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v10 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GuardDutyGetDescribeListPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeImages",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeTransitGatewayAttachments",
        "organizations:ListAccounts",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetEncryptionConfiguration",
        "s3:GetBucketTagging",
        "s3:GetAccountPublicAccessBlock",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "lambda:GetFunctionConfiguration",
        "lambda:ListTags",
        "eks:ListClusters",
        "eks:DescribeCluster",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "ecs:ListClusters",
        "ecs:DescribeClusters"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GuardDutyCreateSLRPolicy",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "malware-protection.guardduty.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "GuardDutyCreateVpcEndpointPolicy",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "GuardDutyManaged"
        },
        "StringLike" : {
          "ec2:VpceServiceName" : [
            "com.amazonaws.*.guardduty-data",
            "com.amazonaws.*.guardduty-data-fips"
          ]
        }
      }
    },
    {
      "Sid" : "GuardDutyModifyDeleteVpcEndpointPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint",
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/GuardDutyManaged" : false
        }
      }
```

```
    },
    {
      "Sid" : "GuardDutyCreateModifyVpcEndpointNetworkPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Sid" : "GuardDutyCreateTagsDuringVpcEndpointCreationPolicy",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "GuardDutyManaged"
        }
      }
    },
    {
      "Sid" : "GuardDutySecurityGroupManagementPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/GuardDutyManaged" : false
        }
      }
```

```
    },
    {
      "Sid" : "GuardDutyCreateSecurityGroupPolicy",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSecurityGroup",
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/GuardDutyManaged" : "*"
        }
      }
    },
    {
      "Sid" : "GuardDutyCreateSecurityGroupForVpcPolicy",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSecurityGroup",
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Sid" : "GuardDutyCreateTagsDuringSecurityGroupCreationPolicy",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateSecurityGroup"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "GuardDutyManaged"
        }
      }
    },
    {
      "Sid" : "GuardDutyCreateEksAddonPolicy",
      "Effect" : "Allow",
      "Action" : "eks:CreateAddon",
      "Resource" : "arn:aws:eks:*:*:cluster/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "GuardDutyManaged"
        }
      }
    },
    {
```

```
      "Sid" : "GuardDutyEksAddonManagementPolicy",
      "Effect" : "Allow",
      "Action" : [
        "eks:DeleteAddon",
        "eks:UpdateAddon",
        "eks:DescribeAddon"
      ],
      "Resource" : "arn:aws:eks:*:*:addon/*/aws-guardduty-agent/*"
    },
    {
      "Sid" : "GuardDutyEksClusterTagResourcePolicy",
      "Effect" : "Allow",
      "Action" : "eks:TagResource",
      "Resource" : "arn:aws:eks:*:*:cluster/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "GuardDutyManaged"
        }
      }
    },
    {
      "Sid" : "GuardDutyEcsPutAccountSettingsDefaultPolicy",
      "Effect" : "Allow",
      "Action" : "ecs:PutAccountSettingDefault",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ecs:account-setting" : [
            "guardDutyActivate"
          ]
        }
      }
    },
    {
      "Sid" : "SsmCreateDescribeUpdateDeleteStartAssociationPermission",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAssociation",
        "ssm:DeleteAssociation",
        "ssm:UpdateAssociation",
        "ssm:CreateAssociation",
        "ssm:StartAssociationsOnce"
      ],
      "Resource" : "arn:aws:ssm:*:*:association/*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/GuardDutyManaged" : "true"
        }
      }
    },
    {
      "Sid" : "SsmAddTagsToResourcePermission",
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:association/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "GuardDutyManaged"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/GuardDutyManaged" : "true"
        }
      }
    },
    {
      "Sid" : "SsmCreateUpdateAssociationInstanceDocumentPermission",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:UpdateAssociation"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/AmazonGuardDuty-
ConfigureRuntimeMonitoringSsmPlugin"
    },
    {
      "Sid" : "SsmSendCommandPermission",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:document/AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin"
      ]
    },
    {
```

```
      "Sid" : "SsmGetCommandStatus",
      "Effect" : "Allow",
      "Action" : "ssm:GetCommandInvocation",
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonHealthLakeFullAccess

説明: Amazon HealthLake サービスへのフルアクセスを提供します。

AmazonHealthLakeFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonHealthLakeFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 2 月 17 日 01:07 UTC
- 編集日時: 2021 年 2 月 17 日 01:07 UTC
- ARN: arn:aws:iam::aws:policy/AmazonHealthLakeFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonHealthLakeReadOnlyAccess

説明: Amazon HealthLake サービスへの読み取り専用アクセスを提供します。

AmazonHealthLakeReadOnlyAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonHealthLakeReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 2 月 17 日 02:43 UTC
- 編集日時: 2021 年 2 月 17 日 02:43 UTC
- ARN: arn:aws:iam::aws:policy/AmazonHealthLakeReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonHoneycodeFullAccess

説明: AWS マネジメントコンソール および SDK 経由で Honeycode へのフルアクセスを提供します。

AmazonHoneycodeFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonHoneycodeFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 6 月 24 日 20:28 UTC
- 編集日時: 2020 年 6 月 24 日 20:28 UTC
- ARN: arn:aws:iam::aws:policy/AmazonHoneycodeFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonHoneycodeReadOnlyAccess

説明: AWS マネジメントコンソール および SDK 経由で Honeycode への読み取り専用アクセスを提供します。

`AmazonHoneycodeReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonHoneycodeReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 6 月 24 日 20:28 UTC
- 編集日時: 2020 年 12 月 1 日 17:27 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonHoneycodeServiceRolePolicy

説明 Amazon Honeycode がリソースにアクセスする際に必要なサービスリンクロール。

AmazonHoneycodeServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 11 月 18 日 18:03 UTC
- 編集日時: 2020 年 11 月 18 日 18:03 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonHoneycodeServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonHoneycodeTeamAssociationFullAccess

説明: AWS マネジメントコンソール および SDK 経由で Honeycode Team Association へのフルアクセスを提供します。

AmazonHoneycodeTeamAssociationFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonHoneycodeTeamAssociationFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 6 月 24 日 20:28 UTC
- 編集日時: 2020 年 6 月 24 日 20:28 UTC
- ARN: arn:aws:iam::aws:policy/AmazonHoneycodeTeamAssociationFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
  "Statement" : [
    {
      "Action" : [
        "honeycode:ListTeamAssociations",
        "honeycode:ApproveTeamAssociation",
        "honeycode:RejectTeamAssociation"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonHoneycodeTeamAssociationReadOnlyAccess

説明: AWS マネジメントコンソール および SDK 経由で Honeycode Team Association への読み取り専用アクセスを提供します。

`AmazonHoneycodeTeamAssociationReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonHoneycodeTeamAssociationReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 6 月 24 日 20:27 UTC
- 編集日時: 2020 年 6 月 24 日 20:27 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonHoneycodeWorkbookFullAccess

説明: AWS マネジメントコンソール および SDK 経由で Honeycode Workbook へのフルアクセスを提供します。

`AmazonHoneycodeWorkbookFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonHoneycodeWorkbookFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 6 月 24 日 20:28 UTC
- 編集日時: 2020 年 12 月 1 日 17:30 UTC
- ARN: arn:aws:iam::aws:policy/AmazonHoneycodeWorkbookFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonHoneycodeWorkbookReadOnlyAccess

説明: AWS マネジメントコンソール および SDK 経由で Honeycode Workbook への読み取り専用アクセスを提供します。

`AmazonHoneycodeWorkbookReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonHoneycodeWorkbookReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 6 月 24 日 20:28 UTC
- 編集日時: 2020 年 12 月 1 日 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeWorkbookReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "honeycode:GetScreenData",
        "honeycode:DescribeTableDataImportJob",
        "honeycode:ListTableColumns",
        "honeycode:ListTableRows",
        "honeycode:ListTables",
        "honeycode:QueryTableRows"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonInspector2AgentlessServiceRolePolicy

説明: エージェントレスセキュリティ評価を実行する AWS のサービス ために必要な へのアクセス権を Amazon Inspector に付与します

`AmazonInspector2AgentlessServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 11 月 20 日 15:18 UTC
- 編集日時: 2023 年 11 月 20 日 15:18 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspector2AgentlessServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonInspector2FullAccess

説明: Amazon Inspector へのフルアクセスと、組織などの他の関連サービスへのアクセスを提供します。

AmazonInspector2FullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonInspector2FullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 11 月 29 日 19:10 UTC
- 編集日時: 2024 年 4 月 25 日 13:21 UTC
- ARN: arn:aws:iam::aws:policy/AmazonInspector2FullAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonInspector2FullAccess_v2

説明: Amazon Inspector へのフルアクセスと、Organizations などの他の関連サービスへのアクセスを制限付き組織アクセスで提供します。

`AmazonInspector2FullAccess_v2` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonInspector2FullAccess_v2` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 7 月 3 日 16:07 UTC
- 編集日時: 2025 年 11 月 14 日 23:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspector2FullAccess_v2`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowFullAccessToInspectorApis",
      "Effect" : "Allow",
      "Action" : "inspector2:*",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAccessToCodeGuruApis",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-security:BatchGetFindings",
        "codeguru-security:GetAccountConfiguration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAccessToCreateSlr",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "agentless.inspector2.amazonaws.com",
            "inspector2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowServicePrincipalBasedAccessToOrganizationApis",
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
```

```
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "inspector2.amazonaws.com",
            "agentless.inspector2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowOrganizationalBasedAccessToOrganizationApis",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganizationalUnit"
      ],
      "Resource" : "arn:aws:organizations::*:ou/o-*/ou-*"
    },
    {
      "Sid" : "AllowAccountsBasedAccessToOrganizationApis",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount"
      ],
      "Resource" : "arn:aws:organizations::*:account/o-*/*"
    },
    {
      "Sid" : "AllowAccessToOrganizationApis",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowListPoliciesForInspectorPolicyType",
      "Effect" : "Allow",
      "Action" : "organizations:ListPolicies",
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "organizations:PolicyType" : [
            "INSPECTOR_POLICY"
          ]
        }
      }
    },
    {
      "Sid" : "AllowDescribeResourcePolicyForDelegation",
      "Effect" : "Allow",
      "Action" : "organizations:DescribeResourcePolicy",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowDescribeEffectivePolicyForInspector",
      "Effect" : "Allow",
      "Action" : "organizations:DescribeEffectivePolicy",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:PolicyType" : [
            "INSPECTOR_POLICY"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonInspector2ManagedCisPolicy

説明: これは、CIS スキャンのインスペクターサービスと通信するために、お客様が各自の口ールにアタッチする必要があるマネージドポリシーです。

AmazonInspector2ManagedCisPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonInspector2ManagedCisPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 1 月 24 日 16:31 UTC
- 編集日時: 2024 年 1 月 24 日 16:31 UTC
- ARN: arn:aws:iam::aws:policy/AmazonInspector2ManagedCisPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PermissionsForCISScans",
      "Effect" : "Allow",
      "Action" : [
        "inspector2:StartCisSession",
        "inspector2:StopCisSession",
        "inspector2:SendCisSessionTelemetry",
        "inspector2:SendCisSessionHealth"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonInspector2ReadOnlyAccess

説明: Amazon inspector2 サービスと関連するサポートサービスへの読み取り専用アクセスを提供します

`AmazonInspector2ReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonInspector2ReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 1 月 21 日 14:45 UTC
- 編集日時: 2025 年 11 月 14 日 23:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspector2ReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "inspector2:BatchGet*",
        "inspector2:List*",
        "inspector2:Describe*",
        "inspector2:Get*",
        "inspector2:Search*",
        "codeguru-security:BatchGetFindings",
        "codeguru-security:GetAccountConfiguration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowListPoliciesForInspectorPolicyType",
      "Effect" : "Allow",
      "Action" : "organizations:ListPolicies",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:PolicyType" : [
            "INSPECTOR_POLICY"
          ]
        }
      }
    },
    {
      "Sid" : "AllowDescribeResourcePolicyForDelegation",
      "Effect" : "Allow",
      "Action" : "organizations:DescribeResourcePolicy",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowDescribeEffectivePolicyForInspector",
      "Effect" : "Allow",
      "Action" : "organizations:DescribeEffectivePolicy",
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "organizations:PolicyType" : [
            "INSPECTOR_POLICY"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonInspector2ServiceRolePolicy

説明: セキュリティ評価の実行 AWS のサービス に必要な へのアクセス権を Amazon Inspector に付与します

`AmazonInspector2ServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 11 月 16 日 20:27 UTC
- 編集日時: 2025 年 11 月 10 日 18:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspector2ServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v17 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TirosPolicy",
      "Effect" : "Allow",
      "Action" : [
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAssociations",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualGateways",
        "directconnect:DescribeVirtualInterfaces",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGatewayVpcAttachments",
```

```
        "ec2:DescribeTransitGateways",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:SearchTransitGatewayRoutes",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetHealth",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups",
        "tiros:CreateQuery",
        "tiros:GetQueryAnswer"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "PackageVulnerabilityScanning",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchGetImage",
        "ecr:BatchGetRepositoryScanningConfiguration",
        "ecr:DescribeImages",
        "ecr:DescribeRegistry",
        "ecr:DescribeRepositories",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer",
        "ecr:GetRegistryScanningConfiguration",
```

```
        "ecr:ListImages",
        "ecr:PutRegistryScanningConfiguration",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "ssm:DescribeAssociation",
        "ssm:DescribeAssociationExecutions",
        "ssm:DescribeInstanceInformation",
        "ssm:ListAssociations",
        "ssm:ListResourceDataSync"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LambdaPackageVulnerabilityScanning",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions",
        "lambda:GetFunction",
        "lambda:GetLayerVersion",
        "lambda:ListTags",
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GatherInventory",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:StartAssociationsOnce",
        "ssm:UpdateAssociation"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:document/AmazonInspector2-*",
        "arn:aws:ssm:*:*:document/AWS-GatherSoftwareInventory",
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*:*:association/*"
      ]
    },
    {
      "Sid" : "GatherInventoryDeleteAssociation",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ssm:DeleteAssociation"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:association/*"
      ]
    },
    {
      "Sid" : "DataSyncCleanup",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateResourceDataSync",
        "ssm:DeleteResourceDataSync"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:resource-data-sync/InspectorResourceDataSync-do-not-delete"
      ]
    },
    {
      "Sid" : "ManagedRules",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:DeleteRule",
        "events:DescribeRule",
        "events:ListTargetsByRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/DO-NOT-DELETE-AmazonInspector*ManagedRule"
      ]
    },
    {
      "Sid" : "LambdaCodeVulnerabilityScanning",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-security:CreateScan",
        "codeguru-security:GetAccountConfiguration",
        "codeguru-security:GetFindings",
        "codeguru-security:GetScan",
        "codeguru-security:ListFindings",
        "codeguru-security:BatchGetFindings",
        "codeguru-security:DeleteScansByCategory"
```

```
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CodeGuruCodeVulnerabilityScanning",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:ListAttachedRolePolicies",
        "iam:ListPolicies",
        "iam:ListPolicyVersions",
        "iam:ListRolePolicies",
        "lambda:ListVersionsByFunction"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "codeguru-security.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "Ec2DeepInspection",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter",
        "ssm:GetParameters",
        "ssm:DeleteParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/inspector-aws/service/inspector-linux-application-
paths"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowManagementOfServiceLinkedChannel",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateServiceLinkedChannel",
        "cloudtrail:DeleteServiceLinkedChannel"
      ],
      "Resource" : [
        "arn:aws:cloudtrail:*:*:channel/aws-service-channel/inspector2/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowListServiceLinkedChannels",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:ListServiceLinkedChannels"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowToRunInvokeCisSpecificDocuments",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AmazonInspector2-InvokeInspectorSsmPluginCIS"
```

```
      ]
    },
    {
      "Sid" : "AllowToRunCisCommandsToSpecificResources",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowToPutCloudwatchMetricData",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Inspector2"
        }
      }
    },
    {
      "Sid" : "AllowListAccessToECSAndEKS",
      "Effect" : "Allow",
      "Action" : [
        "ecs:ListClusters",
        "ecs:ListTasks",
        "eks:ListClusters"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowAccessToECSTasks",
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeTasks"
      ],
      "Resource" : "arn:aws:ecs:*:*:task/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowInspectorEnablementForAwsOrgPolicy",
      "Effect" : "Allow",
      "Action" : [
        "inspector2:Enable",
        "inspector2:Disable",
        "inspector2:EnableDelegatedAdminAccount",
        "inspector2:AssociateMember"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowInspectorServiceDelegatedAdminFromAwsOrg",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "organizations:ServicePrincipal" : [
            "agentless.inspector2.amazonaws.com",
            "inspector2.amazonaws.com"
          ]
        }
      }
```

```
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonInspectorFullAccess

説明: Amazon Inspector へのフルアクセスを提供します。

`AmazonInspectorFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonInspectorFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 10 月 7 日 17:08 UTC
- 編集日時: 2017 年 12 月 21 日 14:53 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspectorFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonInspectorReadOnlyAccess

説明: Amazon Inspector への読み取り専用アクセスを提供します。

`AmazonInspectorReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonInspectorReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 10 月 7 日 17:08 UTC
- 編集日時: 2019 年 10 月 1 日 15:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspectorReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
```

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonInspectorServiceRolePolicy

説明: セキュリティ評価の実行 AWS のサービス に必要な へのアクセス権を Amazon Inspector に付与します

AmazonInspectorServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 11 月 21 日 15:48 UTC
- 編集日時: 2020 年 9 月 11 日 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspectorServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonKendraFullAccess

説明: 経由で Amazon Kendra へのフルアクセスを提供します AWS マネジメントコンソール。

AmazonKendraFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonKendraFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 12 月 3 日 16:15 UTC
- 編集日時: 2019 年 12 月 3 日 16:15 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKendraFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonKendraReadOnlyAccess

説明: 経由で Amazon Kendra への読み取り専用アクセスを提供します AWS マネジメントコンソール。

`AmazonKendraReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonKendraReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 12 月 3 日 16:13 UTC
- 編集日時: 2021 年 5 月 27 日 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKendraReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonKeyspacesFullAccess

説明: Amazon Keyspaces へのフルアクセスを提供します

AmazonKeyspacesFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonKeyspacesFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 4 月 23 日 17:06 UTC
- 編集日時: 2025 年 6 月 30 日 17:37 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKeyspacesFullAccess

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CassandraFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "cassandra:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ApplicationAutoscalingFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeleteScheduledAction",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
```

```
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "application-autoscaling:PutScheduledAction",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget",
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudwatchAlarmsFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ApplicationAutoscalingServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/cassandra.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_CassandraTable",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "cassandra.application-autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "KeyspacesReplicationServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
replication.cassandra.amazonaws.com/AWSServiceRoleForKeyspacesReplication",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "replication.cassandra.amazonaws.com"
        }
```

```
      }
    },
    {
      "Sid" : "KeyspacesCDCServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/cassandra-
streams.amazonaws.com/AWSServiceRoleForAmazonKeyspacesCDC",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "cassandra-streams.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "Ec2VpcReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonKeyspacesReadOnlyAccess

説明: Amazon Keyspaces への読み取り専用アクセスを提供

`AmazonKeyspacesReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonKeyspacesReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 4 月 23 日 17:07 UTC
- 編集日時: 2025 年 6 月 30 日 17:37 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKeyspacesReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cassandra:Select",
        "cassandra:ListStreams",
        "cassandra:GetStream",
        "cassandra:GetShardIterator",
        "cassandra:GetRecords"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
```

```
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonKeyspacesReadOnlyAccess_v2

説明: Amazon Keyspaces および関連 AWS サービスへの読み取り専用アクセスを提供します。

AmazonKeyspacesReadOnlyAccess_v2 は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonKeyspacesReadOnlyAccess_v2 をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 9 月 12 日 17:01 UTC
- 編集日時: 2025 年 6 月 27 日 22:22 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKeyspacesReadOnlyAccess_v2

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cassandra:Select",
        "cassandra:ListStreams",
        "cassandra:GetStream",
        "cassandra:GetShardIterator",
        "cassandra:GetRecords"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcEndpoints"
```

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonKinesisAnalyticsFullAccess

説明: 経由で Amazon Kinesis Analytics へのフルアクセスを提供します AWS マネジメントコンソール。

`AmazonKinesisAnalyticsFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonKinesisAnalyticsFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2016 年 9 月 21 日 19:01 UTC
- 編集日時: 2016 年 9 月 21 日 19:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisAnalyticsFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonKinesisAnalyticsReadOnly

説明: 経由で Amazon Kinesis Analytics への読み取り専用アクセスを提供します AWS マネジメントコンソール。

`AmazonKinesisAnalyticsReadOnly` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonKinesisAnalyticsReadOnly` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2016 年 9 月 21 日 18:16 UTC
- 編集日時: 2016 年 9 月 21 日 18:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisAnalyticsReadOnly`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonKinesisFirehoseFullAccess

説明: すべての Amazon Kinesis Firehose デリバリーストリームへのフルアクセスを提供します。

`AmazonKinesisFirehoseFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonKinesisFirehoseFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 10 月 7 日 18:45 UTC
- 編集日時: 2015 年 10 月 7 日 18:45 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKinesisFirehoseFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する

- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonKinesisFirehoseReadOnlyAccess

説明: すべての Amazon Kinesis Firehose デリバリーストリームへの読み取り専用アクセスを提供します。

`AmazonKinesisFirehoseReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonKinesisFirehoseReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 10 月 7 日 18:43 UTC
- 編集日時: 2015 年 10 月 7 日 18:43 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisFirehoseReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
      "Action" : [
        "firehose:Describe*",
        "firehose:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonKinesisFullAccess

説明: 経由ですべてのストリームへのフルアクセスを提供します AWS マネジメントコンソール。

`AmazonKinesisFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonKinesisFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2015 年 2 月 6 日 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonKinesisReadOnlyAccess

説明: 経由ですべてのストリームへの読み取り専用アクセスを提供します AWS マネジメントコンソール。

`AmazonKinesisReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonKinesisReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2015 年 2 月 6 日 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonKinesisVideoStreamsFullAccess

説明: 経由で Amazon Kinesis Video Streams へのフルアクセスを提供します AWS マネジメントコンソール。

AmazonKinesisVideoStreamsFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonKinesisVideoStreamsFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 12 月 1 日 23:27 UTC
- 編集日時: 2017 年 12 月 1 日 23:27 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKinesisVideoStreamsFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonKinesisVideoStreamsReadOnlyAccess

説明: 経由で AWS Kinesis Video Streams への読み取り専用アクセスを提供します AWS マネジメントコンソール。

`AmazonKinesisVideoStreamsReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonKinesisVideoStreamsReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 12 月 1 日 23:14 UTC
- 編集日時: 2017 年 12 月 1 日 23:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisVideoStreamsReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
```

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonLaunchWizard_Fullaccess

説明: AWS 起動ウィザードおよびその他の必要なサービスへのフルアクセス。

AmazonLaunchWizard_Fullaccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonLaunchWizard_Fullaccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 8 月 6 日 17:47 UTC
- 編集日時: 2023 年 2 月 22 日 17:25 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLaunchWizard_Fullaccess

ポリシーのバージョン

ポリシーのバージョン: v15 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonLaunchWizardFullAccessV2

説明: AWS 起動ウィザードおよびその他の必要なサービスへのフルアクセス。

AmazonLaunchWizardFullAccessV2 は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonLaunchWizardFullAccessV2 をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 9 月 1 日 17:14 UTC
- 編集日時: 2023 年 9 月 1 日 17:14 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLaunchWizardFullAccessV2

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonLexChannelsAccess

説明: このポリシーにより、顧客はチャネルから Lex ランタイムを呼び出すことができます

AmazonLexChannelsAccess は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 1 月 13 日 20:12 UTC
- 編集日時: 2021 年 1 月 13 日 20:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonLexChannelsAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する

- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonLexFullAccess

説明: 経由で Amazon Lex へのフルアクセスを提供します AWS マネジメントコンソール。また、Lex サービスにリンクされたロールを作成し、限定された Lambda 関数セットを呼び出すための Lex アクセス許可を付与するためのアクセスも提供します。

`AmazonLexFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonLexFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 4 月 11 日 23:20 UTC
- 編集日時: 2024 年 4 月 16 日 20:06 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLexFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v9 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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"
```

```
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonLexReadOnly

説明: Amazon Lex への読み取り専用アクセスを提供します。

`AmazonLexReadOnly` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonLexReadOnly` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 4 月 11 日 23:13 UTC
- 編集日時: 2024 年 5 月 13 日 16:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLexReadOnly`

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonLexReplicationPolicy

説明: Amazon Lex がユーザーに代わってリージョン間で Lex リソースをレプリケートできるようにします。

`AmazonLexReplicationPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2024 年 1 月 31 日 23:29 UTC
- 編集日時: 2025 年 6 月 24 日 21:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonLexReplicationPolicy`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReplicationServicePolicyStatement1",
      "Effect" : "Allow",
      "Action" : [
        "lex:BuildBotLocale",
        "lex:ListBotLocales",
        "lex:CreateBotAlias",
        "lex:UpdateBotAlias",
        "lex:DeleteBotAlias",
        "lex:DescribeBotAlias",
        "lex:CreateBotVersion",
        "lex:DeleteBotVersion",
        "lex:DescribeBotVersion",
        "lex:CreateExport",
```

```
        "lex:DescribeBot",
        "lex:UpdateExport",
        "lex:DescribeExport",
        "lex:DescribeBotLocale",
        "lex:DescribeIntent",
        "lex:ListIntents",
        "lex:DescribeSlotType",
        "lex:ListSlotTypes",
        "lex:DescribeSlot",
        "lex:ListSlots",
        "lex:DescribeCustomVocabulary",
        "lex:StartImport",
        "lex:DescribeImport",
        "lex:CreateBot",
        "lex:UpdateBot",
        "lex:DeleteBot",
        "lex:CreateBotLocale",
        "lex:UpdateBotLocale",
        "lex:DeleteBotLocale",
        "lex:CreateIntent",
        "lex:UpdateIntent",
        "lex:DeleteIntent",
        "lex:CreateSlotType",
        "lex:UpdateSlotType",
        "lex:DeleteSlotType",
        "lex:CreateSlot",
        "lex:UpdateSlot",
        "lex:DeleteSlot",
        "lex:CreateCustomVocabulary",
        "lex:UpdateCustomVocabulary",
        "lex:DeleteCustomVocabulary",
        "lex:DeleteBotChannel",
        "lex:ListTagsForResource",
        "lex:TagResource",
        "lex:UntagResource",
        "lex:CreateResourcePolicy",
        "lex:DeleteResourcePolicy",
        "lex:DescribeResourcePolicy",
        "lex:UpdateResourcePolicy"
      ],
      "Resource" : [
        "arn:aws:lex:*:*:bot/*",
        "arn:aws:lex:*:*:bot-alias/*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ReplicationServicePolicyStatement2",
      "Effect" : "Allow",
      "Action" : [
        "lex:CreateUploadUrl",
        "lex:ListBots"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ReplicationServicePolicyStatement3",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "lexv2.amazonaws.com"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonLexRunBotsOnly

説明: Amazon Lex 会話型 API へのアクセスを提供します。

AmazonLexRunBotsOnly は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonLexRunBotsOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 4 月 11 日 23:06 UTC
- 編集日時: 2021 年 8 月 18 日 00:15 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLexRunBotsOnly

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonLexV2BotPolicy

説明: Lex V2 ボットがユーザーに代わって他の AWS サービスを呼び出すためのアクセスを提供します。

AmazonLexV2BotPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 1 月 13 日 20:10 UTC
- 編集日時: 2021 年 1 月 13 日 20:10 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonLexV2BotPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonLookoutEquipmentFullAccess

説明: Amazon Lookout for Equipment オペレーションへのフルアクセスを提供します

`AmazonLookoutEquipmentFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonLookoutEquipmentFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2021 年 4 月 8 日 15:52 UTC
- 編集日時: 2021 年 11 月 24 日 21:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutEquipmentFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonLookoutEquipmentReadOnlyAccess

説明: Amazon Lookout for Equipment への読み取り専用アクセスを提供します

AmazonLookoutEquipmentReadOnlyAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonLookoutEquipmentReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 5 月 5 日 16:47 UTC
- 編集日時: 2022 年 11 月 10 日 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutEquipmentReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonLookoutMetricsFullAccess

説明: Amazon Lookout for Metrics のすべてのアクションへのアクセスを許可

AmazonLookoutMetricsFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonLookoutMetricsFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 5 月 7 日 00:43 UTC
- 編集日時: 2021 年 5 月 7 日 00:43 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLookoutMetricsFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonLookoutMetricsReadOnlyAccess

説明: Amazon Lookout for Metrics のすべての読み取り専用アクションへのアクセスを許可

`AmazonLookoutMetricsReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonLookoutMetricsReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 5 月 7 日 00:43 UTC
- 編集日時: 2022 年 1 月 4 日 18:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutMetricsReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonLookoutVisionConsoleFullAccess

説明: Amazon Lookout for Vision へのフルアクセスと、必要なサービスとコンソールの依存関係へのスコープ付きアクセスを提供します。

AmazonLookoutVisionConsoleFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonLookoutVisionConsoleFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 5 月 11 日 19:37 UTC
- 編集日時: 2021 年 5 月 11 日 19:37 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLookoutVisionConsoleFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonLookoutVisionConsoleReadOnlyAccess

説明: Amazon Lookout for Vision への読み取り専用アクセスと、必要なサービスとコンソールの依存関係へのスコープ付きアクセスを提供します。

`AmazonLookoutVisionConsoleReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonLookoutVisionConsoleReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 5 月 11 日 19:32 UTC
- 編集日時: 2021 年 12 月 9 日 02:46 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutVisionConsoleReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonLookoutVisionFullAccess

説明: Amazon Lookout for Vision へのフルアクセスと、必要な依存関係へのスコープ付きアクセスを提供します。

`AmazonLookoutVisionFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonLookoutVisionFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 5 月 11 日 19:24 UTC
- 編集日時: 2021 年 5 月 11 日 19:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutVisionFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonLookoutVisionReadOnlyAccess

説明: Amazon Lookout for Vision への読み取り専用アクセスと、必要な依存関係へのスコープ付きアクセスを提供します。

`AmazonLookoutVisionReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonLookoutVisionReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2021 年 5 月 11 日 19:11 UTC
- 編集日時: 2021 年 12 月 9 日 03:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutVisionReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonMachineLearningBatchPredictionsAccess

説明: Amazon Machine Learning のバッチ予測をリクエストするアクセス許可をユーザーに付与します。

AmazonMachineLearningBatchPredictionsAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonMachineLearningBatchPredictionsAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 4 月 9 日 17:12 UTC
- 編集日時: 2015 年 4 月 9 日 17:12 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMachineLearningBatchPredictionsAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:CreateBatchPrediction",
        "machinelearning:DeleteBatchPrediction",
        "machinelearning:DescribeBatchPredictions",
        "machinelearning:GetBatchPrediction",
        "machinelearning:UpdateBatchPrediction"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonMachineLearningCreateOnlyAccess

説明: 予測以外の Amazon Machine Learning リソースの作成アクセスを提供します。

`AmazonMachineLearningCreateOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonMachineLearningCreateOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 4 月 9 日 17:18 UTC
- 編集日時: 2016 年 6 月 29 日 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningCreateOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:Add*",
        "machinelearning:Create*",
        "machinelearning:Delete*",
        "machinelearning:Describe*",
        "machinelearning:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonMachineLearningFullAccess

説明: Amazon Machine Learning リソースへのフルアクセスを提供します。

`AmazonMachineLearningFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonMachineLearningFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 4 月 9 日 17:25 UTC
- 編集日時: 2015 年 4 月 9 日 17:25 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMachineLearningFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonMachineLearningManageRealTimeEndpointOnlyAccess

説明: Amazon Machine Learning モデルのリアルタイムエンドポイントを作成および削除するアクセス許可をユーザーに付与します。

AmazonMachineLearningManageRealTimeEndpointOnlyAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonMachineLearningManageRealTimeEndpointOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 4 月 9 日 17:32 UTC
- 編集日時: 2015 年 4 月 9 日 17:32 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMachineLearningManageRealTimeEndpointOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:CreateRealtimeEndpoint",
        "machinelearning:DeleteRealtimeEndpoint"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonMachineLearningReadOnlyAccess

説明: Amazon Machine Learning リソースへの読み取り専用アクセスを提供します。

`AmazonMachineLearningReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonMachineLearningReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 4 月 9 日 17:40 UTC
- 編集日時: 2015 年 4 月 9 日 17:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonMachineLearningRealTimePredictionOnlyAccess

説明: Amazon Machine Learning のリアルタイム予測をリクエストするアクセス許可をユーザーに付与します。

`AmazonMachineLearningRealTimePredictionOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonMachineLearningRealTimePredictionOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 4 月 9 日 17:44 UTC
- 編集日時: 2015 年 4 月 9 日 17:44 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningRealTimePredictionOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonMachineLearningRoleforRedshiftDataSourceV3

説明: Machine Learning が Redshift データソースの Redshift クラスターと S3 ステージング場所を設定して使用できるようにします。

AmazonMachineLearningRoleforRedshiftDataSourceV3 は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonMachineLearningRoleforRedshiftDataSourceV3 をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 6 月 24 日 18:00 UTC
- 編集日時: 2020 年 6 月 24 日 18:00 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonMachineLearningRoleforRedshiftDataSourceV3

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonMacieFullAccess

説明: Amazon Macie へのフルアクセスを提供します。

`AmazonMacieFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonMacieFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 8 月 14 日 14:54 UTC
- 編集日時: 2022 年 7 月 1 日 00:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMacieFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonMacieHandshakeRole

説明: Amazon Macie のサービスにリンクされたロールを作成するためのアクセス許可を付与します。

AmazonMacieHandshakeRole は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonMacieHandshakeRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2018 年 6 月 28 日 15:46 UTC
- 編集日時: 2018 年 6 月 28 日 15:46 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonMacieHandshakeRole

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "iam:AWSServiceName" : "macie.amazonaws.com"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonMacieReadOnlyAccess

説明: Amazon Macie への読み取り専用アクセスを提供します。

`AmazonMacieReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonMacieReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2023 年 6 月 15 日 21:50 UTC
- 編集日時: 2023 年 6 月 15 日 21:50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMacieReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "macie2:Describe*",
        "macie2:Get*",
        "macie2:List*",
        "macie2:BatchGetCustomDataIdentifiers",
        "macie2:SearchResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonMacieServiceRole

説明: データ分析を可能にするため、アカウント内のリソース依存関係への読み取り専用アクセスを Macie に付与します。

AmazonMacieServiceRole は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonMacieServiceRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2017 年 8 月 14 日 14:53 UTC
- 編集日時: 2017 年 8 月 14 日 14:53 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonMacieServiceRole

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "s3:Get*",
        "s3:List*"
      ]
    }
```

```
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonMacieServiceRolePolicy

説明: Amazon Macie のサービスにリンクされたロール

`AmazonMacieServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 6 月 19 日 22:17 UTC
- 編集日時: 2022 年 5 月 19 日 19:16 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonMacieServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonManagedBlockchainConsoleFullAccess

説明: 経由で Amazon Managed Blockchain へのフルアクセスを提供します AWS マネジメントコンソール

`AmazonManagedBlockchainConsoleFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonManagedBlockchainConsoleFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 4 月 29 日 21:23 UTC
- 編集日時: 2019 年 4 月 29 日 21:23 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonManagedBlockchainConsoleFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "managedblockchain:*",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:CreateVpcEndpoint",
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonManagedBlockchainFullAccess

説明: Amazon Managed Blockchain へのフルアクセスを提供します。

AmazonManagedBlockchainFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonManagedBlockchainFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 4 月 29 日 21:39 UTC
- 編集日時: 2019 年 4 月 29 日 21:39 UTC
- ARN: arn:aws:iam::aws:policy/AmazonManagedBlockchainFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonManagedBlockchainReadOnlyAccess

説明: Amazon Managed Blockchain への読み取り専用アクセスを提供します。

`AmazonManagedBlockchainReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonManagedBlockchainReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 4 月 30 日 18:17 UTC
- 編集日時: 2019 年 4 月 30 日 18:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonManagedBlockchainReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
```

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonManagedBlockchainServiceRolePolicy

説明: Amazon Managed Blockchain が使用または管理する AWS のサービス および リソースへのアクセスを有効にします

AmazonManagedBlockchainServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 1 月 17 日 19:51 UTC

- 編集日時: 2020 年 1 月 17 日 19:51 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonManagedBlockchainServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する

- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonMCSFullAccess

説明: Amazon Managed Apache Cassandra Service へのフルアクセスを提供します

AmazonMCSFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonMCSFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 12 月 3 日 13:45 UTC
- 編集日時: 2020 年 4 月 17 日 19:19 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMCSFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonMCSReadOnlyAccess

説明: Amazon Managed Apache Cassandra Service への読み取り専用アクセスを提供します

AmazonMCSReadOnlyAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonMCSReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 12 月 3 日 13:46 UTC
- 編集日時: 2020 年 4 月 17 日 19:21 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMCSReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonMechanicalTurkFullAccess

説明: Amazon Mechanical Turk のすべての API へのフルアクセスを提供します。

`AmazonMechanicalTurkFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonMechanicalTurkFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 12 月 11 日 19:08 UTC
- 編集日時: 2015 年 12 月 11 日 19:08 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonMechanicalTurkReadOnly

説明: Amazon Mechanical Turk の読み取り専用 API へのアクセスを提供します。

AmazonMechanicalTurkReadOnly は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonMechanicalTurkReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 12 月 11 日 19:08 UTC
- 編集日時: 2019 年 9 月 25 日 21:06 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMechanicalTurkReadOnly

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonMemoryDBFullAccess

説明: 経由で Amazon MemoryDB へのフルアクセスを提供します AWS マネジメントコンソール。

`AmazonMemoryDBFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonMemoryDBFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 10 月 8 日 19:24 UTC
- 編集日時: 2021 年 10 月 8 日 19:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMemoryDBFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonMemoryDBReadOnlyAccess

説明: 経由で Amazon MemoryDB への読み取り専用アクセスを提供します AWS マネジメントコンソール。

AmazonMemoryDBReadOnlyAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonMemoryDBReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 10 月 8 日 19:27 UTC

- 編集日時: 2021 年 10 月 8 日 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMemoryDBReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonMobileAnalyticsFinancialReportAccess

説明: すべてのアプリケーションリソースの財務データを含むすべてのレポートへの読み取り専用アクセスを提供します。

AmazonMobileAnalyticsFinancialReportAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonMobileAnalyticsFinancialReportAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2015 年 2 月 6 日 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMobileAnalyticsFinancialReportAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonMobileAnalyticsFullAccess

説明: すべてのアプリケーションリソースへのフルアクセスを提供します。

AmazonMobileAnalyticsFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonMobileAnalyticsFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2015 年 2 月 6 日 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMobileAnalyticsFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonMobileAnalyticsNon-financialReportAccess

説明: すべてのアプリケーションリソースの非財務レポートへの読み取り専用アクセスを提供します。

AmazonMobileAnalyticsNon-financialReportAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonMobileAnalyticsNon-financialReportAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2015 年 2 月 6 日 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMobileAnalyticsNon-financialReportAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonMobileAnalyticsWriteOnlyAccess

説明: すべてのアプリケーションリソースのイベントデータを格納するための書き込み専用アクセスを提供します。(SDK 統合に推奨)

`AmazonMobileAnalyticsWriteOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonMobileAnalyticsWriteOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2015 年 2 月 6 日 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMobileAnalyticsWriteOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonMonitronFullAccess

説明: Amazon Monitron を管理するためのフルアクセスを提供します

AmazonMonitronFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonMonitronFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 12 月 2 日 22:40 UTC
- 編集日時: 2022 年 6 月 8 日 16:27 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMonitronFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonMQApiFullAccess

説明: API/SDK 経由で AmazonMQ へのフルアクセスを提供します。

AmazonMQApiFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonMQApiFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 12 月 18 日 20:31 UTC

- 編集日時: 2020 年 11 月 4 日 16:45 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMQApiFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonMQApiReadOnlyAccess

説明: API/SDK 経由で AmazonMQ への読み取り専用アクセスを提供します。

`AmazonMQApiReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonMQApiReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 12 月 18 日 20:31 UTC
- 編集日時: 2018 年 12 月 18 日 20:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMQApiReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mq:Describe*",
        "mq:List*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonMQFullAccess

説明: 経由で AmazonMQ へのフルアクセスを提供します AWS マネジメントコンソール。

AmazonMQFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonMQFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 11 月 28 日 15:28 UTC
- 編集日時: 2020 年 11 月 4 日 16:34 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMQFullAccess

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonMQReadOnlyAccess

説明: 経由で AmazonMQ への読み取り専用アクセスを提供します AWS マネジメントコンソール。

AmazonMQReadOnlyAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonMQReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 11 月 28 日 15:30 UTC
- 編集日時: 2017 年 11 月 28 日 19:02 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMQReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mq:Describe*",
        "mq:List*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
```

```
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonMQServiceRolePolicy

説明: AWS Amazon MQ のサービスにリンクされたロールポリシー

`AmazonMQServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 11 月 4 日 16:07 UTC
- 編集日時: 2020 年 11 月 4 日 16:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonMQServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonMSKConnectReadOnlyAccess

説明: Amazon MSK Connect への読み取り専用アクセスを提供します

AmazonMSKConnectReadOnlyAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonMSKConnectReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 9 月 20 日 10:18 UTC
- 編集日時: 2021 年 10 月 18 日 09:16 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMSKConnectReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonMSKFullAccess

説明: Amazon MSK へのフルアクセスと、その依存関係に必要なその他のアクセス許可を提供すします。

AmazonMSKFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonMSKFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 1 月 14 日 22:07 UTC
- 編集日時: 2023 年 10 月 18 日 11:33 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMSKFullAccess

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonMSKReadOnlyAccess

説明: Amazon MSK への読み取り専用アクセスを提供します

AmazonMSKReadOnlyAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonMSKReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 1 月 14 日 22:28 UTC
- 編集日時: 2019 年 1 月 14 日 22:28 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMSKReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonMWAAServerlessServiceRolePolicy

説明: Amazon Airflow Serverless Service へのアクセスを提供し、ワークフローのネットワークを管理し、ユーザーに代わって他の AWS サービスにアクセスします。

AmazonMWAAServerlessServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2025 年 11 月 15 日 20:34 UTC
- 編集日時: 2025 年 11 月 15 日 20:34 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonMWAAServerlessServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachNetworkInterface",
```

```
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DetachNetworkInterface"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonMWAAServiceRolePolicy

説明: Amazon Managed Workflows for Apache Airflow で使用されるサービスリンクロール。

`AmazonMWAAServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 11 月 24 日 14:13 UTC
- 編集日時: 2022 年 11 月 17 日 00:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonMWAAServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonNimbleStudio-LaunchProfileWorker

説明: このポリシーは、Nimble Studio 起動プロファイルワーカーが必要とするリソースへのアクセス権を付与します。Nimble Studio Builder で作成された EC2 インスタンスにこのポリシーをアタッチします。

`AmazonNimbleStudio-LaunchProfileWorker` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonNimbleStudio-LaunchProfileWorker` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 4 月 28 日 04:47 UTC
- 編集日時: 2021 年 4 月 28 日 04:47 UTC

- ARN: arn:aws:iam::aws:policy/AmazonNimbleStudio-LaunchProfileWorker

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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"
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonNimbleStudio-StudioAdmin

説明: このポリシーは、スタジオ管理者に関連付けられた Amazon Nimble Studio リソースと、他のサービスの関連するスタジオリソースへのアクセス権を付与します。このポリシーをスタジオに関連する管理者ロールにアタッチしてください。

AmazonNimbleStudio-StudioAdmin は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonNimbleStudio-StudioAdmin をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 4 月 28 日 04:47 UTC
- 編集日時: 2023 年 9 月 22 日 17:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonNimbleStudio-StudioAdmin

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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"
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonNimbleStudio-StudioUser

説明: このポリシーは、スタジオユーザーに関連付けられた Amazon Nimble Studio リソースと、他のサービスの関連するスタジオリソースへのアクセス権を付与します。このポリシーをスタジオに関連付けられているユーザーロールにアタッチしてください。

AmazonNimbleStudio-StudioUser は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonNimbleStudio-StudioUser をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 4 月 28 日 04:48 UTC
- 編集日時: 2023 年 9 月 22 日 17:45 UTC
- ARN: arn:aws:iam::aws:policy/AmazonNimbleStudio-StudioUser

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonODBServiceRolePolicy

説明: Oracle Database@ がユーザーに代わって AWS リソースを管理AWS できるようにします。

AmazonODBServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2024 年 11 月 13 日 18:21 UTC
- 編集日時: 2025 年 9 月 29 日 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonODBServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
    },
    {
      "Sid" : "EC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "NM",
      "Effect" : "Allow",
      "Action" : [
        "networkmanager:GetVpcAttachment",
        "networkmanager:ListAttachments"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EB1",
      "Effect" : "Allow",
      "Action" : [
        "events:ActivateEventSource",
        "events:DescribeEventSource"
      ],
      "Resource" : "arn:aws:events:*:*:event-source/aws.partner/odb*"
    },
    {
      "Sid" : "EB2",
      "Effect" : "Allow",
      "Action" : [
        "events:CreateEventBus",
        "events:DescribeEventBus"
      ],
      "Resource" : "arn:aws:events:*:*:event-bus/aws.partner/odb*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonOmicsFullAccess

説明: Amazon Omics およびその他の必要な AWS のサービスへのフルアクセスを提供します。このポリシーにより、ユーザーは RAM 共有の招待を表示して承諾し、ユーザーの AWS アカウント以外のリソースにアクセスすることができます。

AmazonOmicsFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonOmicsFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 2 月 24 日 00:59 UTC
- 編集日時: 2023 年 2 月 24 日 00:59 UTC
- ARN: arn:aws:iam::aws:policy/AmazonOmicsFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonOmicsReadOnlyAccess

説明: Amazon Omics への読み取り専用アクセスを提供します

AmazonOmicsReadOnlyAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonOmicsReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 11 月 29 日 04:17 UTC
- 編集日時: 2022 年 11 月 29 日 04:17 UTC
- ARN: arn:aws:iam::aws:policy/AmazonOmicsReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonOneEnterpriseFullAccess

説明: このポリシーにより、すべての Amazon One Enterprise のリソースとオペレーションへのアクセスを許可する管理者アクセスが付与されます。

`AmazonOneEnterpriseFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonOneEnterpriseFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 11 月 28 日 04:58 UTC
- 編集日時: 2023 年 11 月 28 日 04:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOneEnterpriseFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonOneEnterpriseInstallerAccess

説明: このポリシーは、デバイスのインストールとアクティベーションを許可する制限付き読み取りおよび書き込みアクセスを付与します。

AmazonOneEnterpriseInstallerAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonOneEnterpriseInstallerAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2023 年 11 月 28 日 05:00 UTC
- 編集日時: 2023 年 11 月 28 日 05:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOneEnterpriseInstallerAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "InstallerAccessStatementID",
      "Effect" : "Allow",
      "Action" : [
        "one:CreateDeviceActivationQrCode",
        "one:GetDeviceInstance",
        "one:GetSite",
        "one:GetSiteAddress",
        "one:ListDeviceInstances",
        "one:ListSites"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonOneEnterpriseReadOnlyAccess

説明: このポリシーは、すべての Amazon One Enterprise リソースとオペレーションに対する読み取り専用アクセス許可を付与します。

AmazonOneEnterpriseReadOnlyAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonOneEnterpriseReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 11 月 28 日 04:59 UTC
- 編集日時: 2023 年 11 月 28 日 04:59 UTC
- ARN: arn:aws:iam::aws:policy/AmazonOneEnterpriseReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadOnlyAccessStatementID",
      "Effect" : "Allow",
      "Action" : [
        "one:Get*",
        "one:List*"
      ],
```

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonOpenSearchDashboardsServiceRolePolicy

説明: ユーザーに代わって CloudWatch などの他の AWS サービスにアクセスするための Amazon OpenSearch Dashboards Service へのアクセスを提供します

`AmazonOpenSearchDashboardsServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 12 月 22 日 19:38 UTC
- 編集日時: 2023 年 12 月 22 日 19:38 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchDashboardsServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonOpenSearchDirectQueryGlueCreateAccess

説明: OpenSearch DirectQuery Service がユーザーに代わってリソースを作成するための AWS Glue APIs にアクセスできるようにします。

`AmazonOpenSearchDirectQueryGlueCreateAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonOpenSearchDirectQueryGlueCreateAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 5 月 6 日 12:24 UTC
- 編集日時: 2024 年 5 月 6 日 12:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchDirectQueryGlueCreateAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonOpenSearchDirectQueryGlueCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:CreatePartition",
        "glue:CreateTable",
        "glue:BatchCreatePartition"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonOpenSearchIngestionFullAccess

説明: Amazon OpenSearch Ingestion がユーザーに代わって他の AWS サービスにアクセスできるようにします。

AmazonOpenSearchIngestionFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonOpenSearchIngestionFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 4 月 26 日 18:11 UTC
- 編集日時: 2023 年 4 月 26 日 18:11 UTC
- ARN: arn:aws:iam::aws:policy/AmazonOpenSearchIngestionFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonOpenSearchIngestionReadOnlyAccess

説明: Amazon OpenSearch Ingestion Service への読み取り専用アクセスを提供します

`AmazonOpenSearchIngestionReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonOpenSearchIngestionReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 4 月 26 日 18:09 UTC
- 編集日時: 2023 年 4 月 26 日 18:09 UTC
- ARN: arn:aws:iam::aws:policy/AmazonOpenSearchIngestionReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "osis:GetPipeline",
        "osis:GetPipelineChangeProgress",
        "osis:GetPipelineBlueprint",
        "osis:ListPipelineBlueprints",
        "osis:ListPipelines",
        "osis:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonOpenSearchIngestionServiceRolePolicy

説明: Amazon OpenSearch Ingestion Service がユーザーに代わって他の AWS サービスにアクセスできるようにします。

`AmazonOpenSearchIngestionServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 11 月 18 日 16:49 UTC
- 編集日時: 2025 年 8 月 28 日 18:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchIngestionServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/OSISManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint",
        "ec2:DeleteVpcEndpoints"
```

```
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/OSISManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/OSIS"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonOpenSearchServerlessServiceRolePolicy

説明: Amazon OpenSearch Serverless がユーザーに代わって CloudWatch APIs などの他の AWS サービスにアクセスすることを許可します。

AmazonOpenSearchServerlessServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 11 月 24 日 19:50 UTC
- 編集日時: 2024 年 7 月 25 日 21:19 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchServerlessServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/AOSS"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonOpenSearchServiceCognitoAccess

説明: Amazon Cognito 設定サービスへのアクセスを提供します。

AmazonOpenSearchServiceCognitoAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonOpenSearchServiceCognitoAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 9 月 2 日 06:31 UTC
- 編集日時: 2021 年 12 月 20 日 14:04 UTC
- ARN: arn:aws:iam::aws:policy/AmazonOpenSearchServiceCognitoAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonOpenSearchServiceFullAccess

説明: Amazon OpenSearch Service 設定サービスへのフルアクセスを提供します。

`AmazonOpenSearchServiceFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonOpenSearchServiceFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 9 月 8 日 05:33 UTC
- 編集日時: 2021 年 9 月 8 日 05:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchServiceFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonOpenSearchServiceReadOnlyAccess

説明: Amazon OpenSearch Service 設定サービスへの読み取り専用アクセスを提供します。

`AmazonOpenSearchServiceReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonOpenSearchServiceReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 9 月 8 日 05:38 UTC
- 編集日時: 2021 年 9 月 8 日 05:38 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchServiceReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonOpenSearchServiceRolePolicy

説明: Amazon OpenSearch Service がユーザーに代わって EC2 Networking APIsなどの他の AWS サービスにアクセスできるようにします。

AmazonOpenSearchServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 8 月 26 日 09:27 UTC
- 編集日時: 2025 年 3 月 27 日 22:52 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v9 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Stmt1480452973134",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
```

```
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "Stmt1480452973145",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973144",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    },
    {
      "Sid" : "Stmt1480452973165",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "Stmt1480452973149",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignIpv6Addresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*"
    },
```

```
    {
      "Sid" : "Stmt1480452973150",
      "Effect" : "Allow",
      "Action" : [
        "ec2:UnAssignIpv6Addresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*"
    },
    {
      "Sid" : "Stmt1480452973154",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973164",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973174",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973184",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddListenerCertificates",
        "elasticloadbalancing:RemoveListenerCertificates"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:listener/*"
      ]
    },
    {
```

```
      "Sid" : "Stmt1480452973194",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    },
    {
      "Sid" : "Stmt1480452973195",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeTags"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973196",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973197",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/ES",
            "AWS/OpenSearch"
          ]
        }
      }
    },
    {
      "Sid" : "Stmt1480452973198",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
```

```
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*"
      ]
    },
    {
      "Sid" : "Stmt1480452973199",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/OpenSearchManaged" : "true"
        }
      }
    },
    {
      "Sid" : "Stmt1480452973200",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint",
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/OpenSearchManaged" : "true"
        }
      }
    },
    {
      "Sid" : "Stmt1480452973201",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973202",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "sso:PutApplicationAccessScope",
      "Resource" : "arn:aws:sso::*:application/*/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceOrgID" : "${aws:PrincipalOrgID}"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonPersonalizeFullAccess

説明: AWS マネジメントコンソール および SDK 経由で Amazon Personalize へのフルアクセスを提供します。関連サービス (S3、CloudWatch など) への限定アクセスも提供します。

`AmazonPersonalizeFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonPersonalizeFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2018 年 12 月 4 日 22:24 UTC
- 編集日時: 2019 年 5 月 30 日 23:46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonPersonalizeFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonPollyFullAccess

説明: Amazon Polly サービスとリソースへのフルアクセスを付与します。

`AmazonPollyFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonPollyFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2016 年 11 月 30 日 18:59 UTC
- 編集日時: 2016 年 11 月 30 日 18:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPollyFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonPollyReadOnlyAccess

説明: Amazon Polly リソースに対する読み取り専用アクセスを付与します。

AmazonPollyReadOnlyAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonPollyReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2016 年 11 月 30 日 18:59 UTC
- 編集日時: 2018 年 7 月 17 日 16:41 UTC
- ARN: arn:aws:iam::aws:policy/AmazonPollyReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "polly:DescribeVoices",
        "polly:GetLexicon",
        "polly:GetSpeechSynthesisTask",
        "polly:ListLexicons",
        "polly:ListSpeechSynthesisTasks",
        "polly:SynthesizeSpeech"
```

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonPrometheusConsoleFullAccess

説明: AWS コンソールで AWS Managed Prometheus リソースへのフルアクセスを付与します

`AmazonPrometheusConsoleFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonPrometheusConsoleFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 12 月 15 日 18:11 UTC
- 編集日時: 2025 年 5 月 22 日 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPrometheusConsoleFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetTagValues",
        "tag:GetTagKeys"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aps:CreateWorkspace",
        "aps:DescribeWorkspace",
        "aps:UpdateWorkspaceAlias",
        "aps:DeleteWorkspace",
        "aps:ListWorkspaces",
        "aps:DescribeAlertManagerDefinition",
        "aps:DescribeRuleGroupsNamespace",
        "aps:CreateAlertManagerDefinition",
        "aps:CreateRuleGroupsNamespace",
        "aps:DeleteAlertManagerDefinition",
        "aps:DeleteRuleGroupsNamespace",
        "aps:ListRuleGroupsNamespaces",
        "aps:PutAlertManagerDefinition",
        "aps:PutRuleGroupsNamespace",
        "aps:TagResource",
        "aps:UntagResource",
        "aps:CreateLoggingConfiguration",
        "aps:UpdateLoggingConfiguration",
        "aps:DeleteLoggingConfiguration",
        "aps:DescribeLoggingConfiguration",
        "aps:UpdateWorkspaceConfiguration",
        "aps:DescribeWorkspaceConfiguration",
        "aps:CreateQueryLoggingConfiguration",
```

```
        "aps:UpdateQueryLoggingConfiguration",
        "aps:DeleteQueryLoggingConfiguration",
        "aps:DescribeQueryLoggingConfiguration"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonPrometheusFullAccess

説明: AWS Managed Prometheus リソースへのフルアクセスを付与します

`AmazonPrometheusFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonPrometheusFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 12 月 15 日 18:10 UTC
- 編集日時: 2023 年 11 月 26 日 20:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPrometheusFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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"
```

```
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonPrometheusQueryAccess

説明: AWS Managed Prometheus リソースに対してクエリを実行するアクセス許可を付与します

`AmazonPrometheusQueryAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonPrometheusQueryAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 12 月 19 日 01:02 UTC
- 編集日時: 2020 年 12 月 19 日 01:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPrometheusQueryAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "aps:GetLabels",
        "aps:GetMetricMetadata",
        "aps:GetSeries",
        "aps:QueryMetrics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonPrometheusRemoteWriteAccess

説明: AWS Managed Prometheus ワークスペースへの書き込み専用アクセスを付与します

`AmazonPrometheusRemoteWriteAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonPrometheusRemoteWriteAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2020 年 12 月 19 日 01:04 UTC
- 編集日時: 2020 年 12 月 19 日 01:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPrometheusRemoteWriteAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonPrometheusScraperServiceRolePolicy

説明: Amazon Managed Service for Prometheus Collector によって管理または使用される AWS リソースへのアクセスを提供します

AmazonPrometheusScraperServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 11 月 26 日 14:19 UTC
- 編集日時: 2024 年 4 月 26 日 20:25 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonPrometheusScraperServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する

- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonQDeveloperAccess

説明: Amazon Q とのやり取りを可能にする開発者アクセスを提供します

AmazonQDeveloperAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonQDeveloperAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 7 月 9 日 08:35 UTC
- 編集日時: 2025 年 5 月 12 日 20:22 UTC
- ARN: arn:aws:iam::aws:policy/AmazonQDeveloperAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
        "q:SendMessage",
        "q:GetConversation",
        "q:ListConversations",
        "q:UpdateConversation",
        "q:DeleteConversation",
        "q:PassRequest",
        "q:StartTroubleshootingAnalysis",
        "q:StartTroubleshootingResolutionExplanation",
        "q:GetTroubleshootingResults",
        "q:UpdateTroubleshootingCommandResult",
        "q:GetIdentityMetaData",
        "q:GenerateCodeFromCommands",
        "q:UsePlugin"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCloudControlReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:GetResource",
        "cloudformation:ListResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSetTrustedIdentity",
      "Effect" : "Allow",
      "Action" : [
        "sts:SetContext"
      ],
      "Resource" : "arn:aws:sts::*:self"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonQFullAccess

説明: Amazon Q とのやり取りを可能にするフルアクセスを提供します

AmazonQFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonQFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 11 月 28 日 16:00 UTC
- 編集日時: 2025 年 5 月 12 日 20:22 UTC
- ARN: arn:aws:iam::aws:policy/AmazonQFullAccess

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowAmazonQFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "q:StartConversation",
        "q:SendMessage",
        "q:GetConversation",
        "q:ListConversations",
        "q:UpdateConversation",
        "q:DeleteConversation",
```

```
        "q:PassRequest",
        "q:StartTroubleshootingAnalysis",
        "q:GetTroubleshootingResults",
        "q:StartTroubleshootingResolutionExplanation",
        "q:UpdateTroubleshootingCommandResult",
        "q:GetIdentityMetadata",
        "q:CreateAssignment",
        "q:DeleteAssignment",
        "q:GenerateCodeFromCommands",
        "q:CreatePlugin",
        "q:UpdatePlugin",
        "q:DeletePlugin",
        "q:GetPlugin",
        "q:UsePlugin",
        "q:ListPlugins",
        "q:ListPluginProviders",
        "q:ListTagsForResource",
        "q:UntagResource",
        "q:TagResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCloudControlReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:GetResource",
        "cloudformation:ListResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSetTrustedIdentity",
      "Effect" : "Allow",
      "Action" : [
        "sts:SetContext"
      ],
      "Resource" : "arn:aws:sts::*:self"
    },
    {
      "Sid" : "AllowPassRoleToAmazonQ",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
```

```
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "q.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonQLDBConsoleFullAccess

説明: 経由で Amazon QLDB へのフルアクセスを提供します AWS マネジメントコンソール。

`AmazonQLDBConsoleFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonQLDBConsoleFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 9 月 5 日 18:24 UTC
- 編集日時: 2022 年 11 月 4 日 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonQLDBConsoleFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonQLDBFullAccess

説明: サービス API 経由で Amazon QLDB へのフルアクセスを提供します。

AmazonQLDBFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonQLDBFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 9 月 5 日 18:23 UTC
- 編集日時: 2022 年 11 月 4 日 17:01 UTC
- ARN: arn:aws:iam::aws:policy/AmazonQLDBFullAccess

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonQLDBReadOnly

説明: Amazon QLDB への読み取り専用アクセスを提供します。

`AmazonQLDBReadOnly` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonQLDBReadOnly` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 9 月 5 日 18:19 UTC
- 編集日時: 2021 年 7 月 2 日 02:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonQLDBReadOnly`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonRDSBetaServiceRolePolicy

説明: Amazon RDS がユーザーに代わって AWS リソースを管理できるようにします。

AmazonRDSBetaServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 5 月 2 日 19:41 UTC
- 編集日時: 2024 年 8 月 7 日 00:54 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSBetaServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v9 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AssociateAddress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateCoipPoolPermission",
        "ec2:CreateLocalGatewayRouteTablePermission",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteCoipPoolPermission",
        "ec2:DeleteLocalGatewayRouteTablePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCoipPools",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLocalGatewayRouteTablePermissions",
```

```
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeLocalGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:DisassociateAddress",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifyVpcEndpoint",
        "ec2:ReleaseAddress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeVpcEndpoints",
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/rds/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/rds/*:log-stream:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/DocDB",
            "AWS/Neptune",
            "AWS/RDS",
            "AWS/Usage"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetRandomPassword"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:PutSecretValue",
        "secretsmanager:RotateSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:UpdateSecretVersionStage",
        "secretsmanager:ListSecretVersionIds"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:rds-beta-us-east-1!*"
      ],
      "Condition" : {
        "StringLike" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "rds-beta-us-
east-1"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "secretsmanager:TagResource",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:rds-beta-us-east-1!*",
      "Condition" : {
```

```
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws:rds:primaryDBInstanceArn",
            "aws:rds:primaryDBClusterArn"
          ]
        },
        "StringLike" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "rds-beta-us-
east-1"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonRDSCustomInstanceProfileRolePolicy

説明: Amazon RDS Custom が EC2 インスタンスプロファイルを介してさまざまなオートメーションアクションとデータベース管理タスクを実行できるようにします。

AmazonRDSCustomInstanceProfileRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRDSCustomInstanceProfileRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 2 月 27 日 17:42 UTC
- 編集日時: 2025 年 3 月 20 日 16:22 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRDSCustomInstanceProfileRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ssmAgentPermission1",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ssmAgentPermission2",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetManifest",
        "ssm:PutConfigurePackageResult"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ssmAgentPermission3",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ssm:GetDocument",
        "ssm:DescribeDocument"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/*"
    },
    {
      "Sid" : "ssmAgentPermission4",
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:OpenControlChannel"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ssmAgentPermission5",
      "Effect" : "Allow",
      "Action" : [
        "ec2messages:AcknowledgeMessage",
        "ec2messages:DeleteMessage",
        "ec2messages:FailMessage",
        "ec2messages:GetEndpoint",
        "ec2messages:GetMessages",
        "ec2messages:SendReply"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "createEc2SnapshotPermission1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot",
        "ec2:CreateSnapshots"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "createEc2SnapshotPermission2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot",
        "ec2:CreateSnapshots"
      ],
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "createEc2SnapshotPermission3",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshots",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "createTagForEc2SnapshotPermission",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
```

```
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ],
          "ec2:CreateAction" : [
            "CreateSnapshot",
            "CreateSnapshots"
          ]
        }
      }
    },
    {
      "Sid" : "rdsCustomS3ObjectPermission",
      "Effect" : "Allow",
      "Action" : [
        "s3:putObject",
        "s3:getObject",
        "s3:getObjectVersion",
        "s3:AbortMultipartUpload",
        "s3:ListMultipartUploadParts"
      ],
      "Resource" : [
        "arn:aws:s3:::do-not-delete-rds-custom-*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "rdsCustomS3BucketPermission",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucketVersions",
        "s3:ListBucketMultipartUploads"
      ],
      "Resource" : [
        "arn:aws:s3:::do-not-delete-rds-custom-*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "readSecretsFromCpPermission",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*",
        "arn:aws:secretsmanager:*:*:secret:rds-custom!*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "createSecretsOnDpPermission",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : "custom-oracle-rac"
        }
      }
    },
    {
```

```
      "Sid" : "publishCwMetricsPermission",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "rdscustom/rds-custom-sqlserver-agent",
            "RDSCustomForOracle/Agent"
          ]
        }
      }
    },
    {
      "Sid" : "putEventsToEventBusPermission",
      "Effect" : "Allow",
      "Action" : "events:PutEvents",
      "Resource" : "arn:aws:events:*:*:event-bus/default"
    },
    {
      "Sid" : "cwlUploadPermission",
      "Effect" : "Allow",
      "Action" : [
        "logs:PutRetentionPolicy",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams",
        "logs:CreateLogStream",
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:rds-custom-instance-*"
    },
    {
      "Sid" : "sendMessageToSqsQueuePermission",
      "Effect" : "Allow",
      "Action" : [
        "sqs:SendMessage",
        "sqs:ReceiveMessage",
        "sqs:DeleteMessage",
        "sqs:GetQueueUrl"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:do-not-delete-rds-custom-*"
      ],
      "Condition" : {
```

```
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : "custom-sqlserver"
        }
      }
    },
    {
      "Sid" : "managePrivateIpOnEniPermission",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : "custom-oracle-rac"
        }
      }
    },
    {
      "Sid" : "kmsPermissionWithSecret",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:SecretARN" : [
            "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*",
            "arn:aws:secretsmanager:*:*:secret:rds-custom!*"
          ]
        },
        "StringLike" : {
          "kms:ViaService" : "secretsmanager.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "kmsPermissionWithS3",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
```

```
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : "arn:aws:s3:::do-not-delete-rds-custom-
*"
        },
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonRDSCustomPreviewServiceRolePolicy

説明: Amazon RDS Custom Preview サービスロールポリシー

AmazonRDSCustomPreviewServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 10 月 8 日 21:44 UTC

- 編集日時: 2025 年 8 月 7 日 20:19 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonRDSCustomPreviewServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v9 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ecc1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeRegions",
        "ec2:DescribeSnapshots",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVolumes",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeImages",
        "ec2:DescribeVpcs",
        "ec2:RegisterImage",
        "ec2:DeregisterImage",
        "ec2:DescribeTags",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:SearchTransitGatewayMulticastGroups",
        "ec2:GetTransitGatewayMulticastDomainAssociations",
        "ec2:DescribeTransitGatewayMulticastDomains",
```

```
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ecc2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DisassociateIamInstanceProfile",
        "ec2:AssociateIamInstanceProfile",
        "ec2:ReplaceIamInstanceProfileAssociation",
        "ec2:TerminateInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:RebootInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ecc1scoping",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
```

```
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ecc1scoping2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:ReleaseAddress"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ecc1scoping3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignPrivateIpAddresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "eccRunInstances1",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccRunInstances2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*",
        "arn:aws:ec2:*:*:placement-group/*"
      ]
    },
    {
      "Sid" : "eccRunInstances3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*::snapshot/*"
      ],
      "Condition" : {
        "StringLike" : {
```

```
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac",
            "custom-oracle"
          ]
        }
      }
    },
    {
      "Sid" : "RequireImdsV2",
      "Effect" : "Deny",
      "Action" : "ec2:RunInstances",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringNotEquals" : {
          "ec2:MetadataHttpTokens" : "required"
        },
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccRunInstances3keyPair1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:DeleteKeyPair"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*",
        "arn:aws:ec2:*:*:key-pair/preview-rds-custom!*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "eccKeyPair2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateKeyPair"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*",
        "arn:aws:ec2:*:*:key-pair/preview-rds-custom!*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccNetworkInterface1",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccNetworkInterface2",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "eccNetworkInterface3",
```

```
      "Effect" : "Allow",
      "Action" : "ec2:DeleteNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccCreateTag1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccCreateTag2",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ],
          "ec2:CreateAction" : [
            "CreateKeyPair",
```

```
            "RunInstances",
            "CreateNetworkInterface",
            "CreateVolume",
            "CreateSnapshots",
            "CopySnapshot",
            "AllocateAddress"
          ]
        }
      }
    },
    {
      "Sid" : "eccVolume1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccVolume2",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVolume",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "eccVolume3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVolumeAttribute",
        "ec2:DeleteVolume",
        "ec2:ModifyVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccVolume4snapshot1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume",
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccSnapshot2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshots"
```

```
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccSnapshot3",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshots",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccSnapshotCopySource",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopySnapshot"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/snap-*"
    },
    {
      "Sid" : "eccSnapshotCopyDestination",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopySnapshot"
      ],
```

```
      "Resource" : [
        "arn:aws:ec2:*::snapshot/${*}"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "iam1",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListInstanceProfiles",
        "iam:GetInstanceProfile",
        "iam:GetRole",
        "iam:ListRolePolicies",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "iam2",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/AWSRDSCustom*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "cloudtrail1",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:GetTrailStatus"
```

```
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:trail/do-not-delete-rds-custom-*"
    },
    {
      "Sid" : "cw1",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:EnableAlarmActions",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "cw2",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:TagResource"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "cw3",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
```

```
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:*"
    },
    {
      "Sid" : "ssm1",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:aws:ssm:*:*:document/*"
    },
    {
      "Sid" : "ssm2",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ssm3",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetCommandInvocation",
        "ssm:GetConnectionStatus",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ssm4",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter",
        "ssm:AddTagsToResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/rds/custom-oracle-rac/*",
      "Condition" : {
        "StringLike" : {
```

```
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ssm5",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/rds/custom-oracle-rac/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eb1",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:TagResource"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eb2",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
```

```
        "events:DescribeRule",
        "events:EnableRule",
        "events:ListTargetsByRule",
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:DisableRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eb3",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "events:ManagedBy" : [
            "custom.rds-preview.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "eb4",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:EnableRule",
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:DisableRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
```

```
      "Condition" : {
        "StringLike" : {
          "events:ManagedBy" : [
            "custom.rds-preview.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "eb5",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*"
    },
    {
      "Sid" : "secretmanager1",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource",
        "secretsmanager:CreateSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*",
        "arn:aws:secretsmanager:*:*:secret:preview-rds-custom!*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "secretmanager2",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource",
        "secretsmanager:DescribeSecret",
```

```
        "secretsmanager:DeleteSecret",
        "secretsmanager:PutSecretValue",
        "secretsmanager:RestoreSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*",
        "arn:aws:secretsmanager:*:*:secret:preview-rds-custom!*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "secretmanager3",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:ListSecrets"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "servicequota1",
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "sqs1",
      "Effect" : "Allow",
```

```
      "Action" : [
        "sqs:CreateQueue",
        "sqs:TagQueue"
      ],
      "Resource" : "arn:aws:sqs:*:*:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle"
          ]
        }
      }
    },
    {
      "Sid" : "sqs2",
      "Effect" : "Allow",
      "Action" : [
        "sqs:GetQueueAttributes",
        "sqs:SendMessage",
        "sqs:ReceiveMessage",
        "sqs:DeleteMessage",
        "sqs:DeleteQueue"
      ],
      "Resource" : "arn:aws:sqs:*:*:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonRDSCustomServiceRolePolicy

説明: Amazon RDS Custom がユーザーに代わって AWS リソースを管理できるようにします。

AmazonRDSCustomServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 10 月 8 日 21:39 UTC
- 編集日時: 2025 年 8 月 7 日 20:49 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonRDSCustomServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v13 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "rdscrc",
      "Effect" : "Allow",
      "Action" : [
        "rds:CrossRegionCommunication"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "ecc1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeRegions",
        "ec2:DescribeSnapshots",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVolumes",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeImages",
        "ec2:DescribeVpcs",
        "ec2:RegisterImage",
        "ec2:DeregisterImage",
        "ec2:DescribeTags",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:SearchTransitGatewayMulticastGroups",
        "ec2:GetTransitGatewayMulticastDomainAssociations",
        "ec2:DescribeTransitGatewayMulticastDomains",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ecc2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DisassociateIamInstanceProfile",
        "ec2:AssociateIamInstanceProfile",
        "ec2:ReplaceIamInstanceProfileAssociation",
        "ec2:TerminateInstances",
        "ec2:StartInstances",
```

```
        "ec2:StopInstances",
        "ec2:RebootInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ecc1scoping",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ecc1scoping2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:ReleaseAddress"
      ],
      "Resource" : [
        "*"
      ],
```

```
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ecc1scoping3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignPrivateIpAddresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccRunInstances1",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "eccRunInstances2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*",
        "arn:aws:ec2:*:*:placement-group/*"
      ]
    },
    {
      "Sid" : "eccRunInstances3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*::snapshot/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac",
            "custom-oracle"
          ]
        }
      }
    },
    {
      "Sid" : "eccModifyInstanceAttribute1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyInstanceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-sqlserver"
          ],
          "ec2:Attribute" : "InstanceType"
        }
      }
    },
    {
      "Sid" : "RequireImdsV2",
      "Effect" : "Deny",
      "Action" : "ec2:RunInstances",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringNotEquals" : {
          "ec2:MetadataHttpTokens" : "required"
        },
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccRunInstances3keyPair1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:DeleteKeyPair"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*",
        "arn:aws:ec2:*:*:key-pair/rds-custom!*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "eccKeyPair2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateKeyPair"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*",
        "arn:aws:ec2:*:*:key-pair/rds-custom!*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccNetworkInterface1",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccNetworkInterface2",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "eccNetworkInterface3",
```

```
      "Effect" : "Allow",
      "Action" : "ec2:DeleteNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccCreateTag1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccCreateTag2",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ],
          "ec2:CreateAction" : [
            "CreateKeyPair",
```

```
            "RunInstances",
            "CreateNetworkInterface",
            "CreateVolume",
            "CreateSnapshot",
            "CreateSnapshots",
            "CopySnapshot",
            "AllocateAddress",
            "CopyImage"
          ]
        }
      }
    },
    {
      "Sid" : "eccVolume1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccVolume2",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVolume",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "eccVolume3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVolumeAttribute",
        "ec2:DeleteVolume",
        "ec2:ModifyVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccVolume4snapshot1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume",
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccSnapshot2",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateSnapshot",
        "ec2:CreateSnapshots"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccSnapshot3",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshots",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccSnapshot4",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshot",
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-sqlserver"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "eccSnapshotCopySource",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopySnapshot"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/snap-*"
    },
    {
      "Sid" : "eccSnapshotCopyDestination",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopySnapshot"
      ],
      "Resource" : [
        "arn:aws:ec2:*::snapshot/${*}"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccAmi1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopyImage"
      ],
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*::snapshot/*"
      ]
    },
    {
      "Sid" : "iam1",
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:ListInstanceProfiles",
        "iam:GetInstanceProfile",
        "iam:GetRole",
        "iam:ListRolePolicies",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "iam2",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/AWSRDSCustom*",
        "arn:aws:iam::*:role/service-role/AWSRDSCustom*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "cloudtrail1",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:GetTrailStatus"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:trail/do-not-delete-rds-custom-*"
    },
    {
      "Sid" : "cw1",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:EnableAlarmActions",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:do-not-delete-rds-custom-*",
      "Condition" : {
```

```
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "cw2",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:TagResource"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "cw3",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:*"
    },
    {
      "Sid" : "ssm1",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:aws:ssm:*:*:document/*"
    },
    {
      "Sid" : "ssm2",
      "Effect" : "Allow",
```

```
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ssm3",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetCommandInvocation",
        "ssm:GetConnectionStatus",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ssm4",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter",
        "ssm:AddTagsToResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/rds/custom-oracle-rac/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ssm5",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteParameter"
      ],
```

```
      "Resource" : "arn:aws:ssm:*:*:parameter/rds/custom-oracle-rac/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eb1",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:TagResource"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eb2",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:DescribeRule",
        "events:EnableRule",
        "events:ListTargetsByRule",
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:DisableRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
```

```
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eb3",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "events:ManagedBy" : [
            "custom.rds.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "eb4",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:EnableRule",
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:DisableRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "events:ManagedBy" : [
            "custom.rds.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "eb5",
      "Effect" : "Allow",
      "Action" : [
```

```
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*"
    },
    {
      "Sid" : "secretmanager1",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource",
        "secretsmanager:CreateSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*",
        "arn:aws:secretsmanager:*:*:secret:rds-custom!*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "secretmanager2",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource",
        "secretsmanager:DescribeSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:PutSecretValue",
        "secretsmanager:RestoreSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*",
        "arn:aws:secretsmanager:*:*:secret:rds-custom!*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
```

```
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "secretmanager3",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:ListSecrets"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "sqs1",
      "Effect" : "Allow",
      "Action" : [
        "sqs:CreateQueue",
        "sqs:TagQueue"
      ],
      "Resource" : "arn:aws:sqs:*:*:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-sqlserver",
            "custom-oracle"
          ]
        }
      }
    },
    {
      "Sid" : "sqs2",
      "Effect" : "Allow",
      "Action" : [
        "sqs:GetQueueAttributes",
        "sqs:SendMessage",
```

```
        "sqs:ReceiveMessage",
        "sqs:DeleteMessage",
        "sqs:DeleteQueue"
      ],
      "Resource" : "arn:aws:sqs:*:*:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-sqlserver",
            "custom-oracle"
          ]
        }
      }
    },
    {
      "Sid" : "servicequota1",
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonRDSDataFullAccess

説明: RDS データ API、RDS データベース認証情報用のシークレットストア API、および DB コンソールクエリ管理 API を使用して、 AWS アカウント内の Aurora Serverless クラスターで SQL ステートメントを実行するためのフルアクセスを許可します。

`AmazonRDSDataFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonRDSDataFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 11 月 20 日 21:29 UTC
- 編集日時: 2019 年 11 月 20 日 21:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSDataFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonRDSDirectoryServiceAccess

説明: ドメインに参加している SQL Server DB インスタンスについて、お客様に代わって RDS が Directory Service マネージド AD にアクセスできるようにします。

`AmazonRDSDirectoryServiceAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonRDSDirectoryServiceAccess` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2016 年 2 月 26 日 02:02 UTC
- 編集日時: 2019 年 5 月 15 日 16:51 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonRDSDirectoryServiceAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ds:DescribeDirectories",
        "ds:AuthorizeApplication",
        "ds:UnauthorizeApplication",
        "ds:GetAuthorizedApplicationDetails"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonRDSEnhancedMonitoringRole

説明: RDS 拡張モニタリング用 CloudWatch にアクセスを付与します

AmazonRDSEnhancedMonitoringRole は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRDSEnhancedMonitoringRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 11 月 11 日 19:58 UTC
- 編集日時: 2015 年 11 月 11 日 19:58 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonRDSEnhancedMonitoringRole

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonRDSFullAccess

説明: 経由で Amazon RDS へのフルアクセスを提供します AWS マネジメントコンソール。

`AmazonRDSFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonRDSFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2023 年 8 月 17 日 23:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v14 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonRDSPerformanceInsightsFullAccess

説明: 経由で RDS Performance Insights へのフルアクセスを提供します AWS マネジメントコンソール

`AmazonRDSPerformanceInsightsFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonRDSPerformanceInsightsFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2023 年 8 月 15 日 23:41 UTC
- 編集日時: 2025 年 11 月 20 日 22:04 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRDSPerformanceInsightsFullAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRDSPerformanceInsightsReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "pi:DescribeDimensionKeys",
        "pi:GetDimensionKeyDetails",
        "pi:GetResourceMetadata",
        "pi:GetResourceMetrics",
        "pi:ListAvailableResourceDimensions",
        "pi:ListAvailableResourceMetrics"
      ],
      "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsAnalisysReportFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "pi:CreatePerformanceAnalysisReport",
        "pi:GetPerformanceAnalysisReport",
        "pi:ListPerformanceAnalysisReports",
        "pi:DeletePerformanceAnalysisReport"
      ],
      "Resource" : "arn:aws:pi:*:*:perf-reports/rds/*/*"
    },
```

```
    {
      "Sid" : "AmazonRDSPerformanceInsightsTaggingFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "pi:TagResource",
        "pi:UntagResource",
        "pi:ListTagsForResource"
      ],
      "Resource" : "arn:aws:pi:*:*:*/rds/*"
    },
    {
      "Sid" : "AmazonRDSDescribeInstanceAccess",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "rds:ListTagsForResource",
        "rds:DescribeDBShardGroups"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:db:*",
        "arn:aws:rds:*:*:cluster:*",
        "arn:aws:rds:*:*:shard-group:*"
      ]
    },
    {
      "Sid" : "AmazonCloudWatchReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonRDSPerformanceInsightsReadOnly

説明: RDS Performance Insights の読み取り専用ポリシー

AmazonRDSPerformanceInsightsReadOnly は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRDSPerformanceInsightsReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 4 月 5 日 00:02 UTC
- 編集日時: 2025 年 11 月 20 日 22:19 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRDSPerformanceInsightsReadOnly

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRDSDescribeDBInstances",
      "Effect" : "Allow",
      "Action" : "rds:DescribeDBInstances",
      "Resource" : "arn:aws:rds:*:*:db:*"
```

```
    },
    {
      "Sid" : "AmazonRDSDescribeDBClusters",
      "Effect" : "Allow",
      "Action" : "rds:DescribeDBClusters",
      "Resource" : "arn:aws:rds:*:*:cluster:*"
    },
    {
      "Sid" : "AmazonRDSDescribeDBShardGroups",
      "Effect" : "Allow",
      "Action" : "rds:DescribeDBShardGroups",
      "Resource" : "arn:aws:rds:*:*:shard-group:*"
    },
    {
      "Sid" : "AmazonRDSListTagsForResource",
      "Effect" : "Allow",
      "Action" : "rds:ListTagsForResource",
      "Resource" : [
        "arn:aws:rds:*:*:db:*",
        "arn:aws:rds:*:*:shard-group:*",
        "arn:aws:rds:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsDescribeDimensionKeys",
      "Effect" : "Allow",
      "Action" : "pi:DescribeDimensionKeys",
      "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsGetDimensionKeyDetails",
      "Effect" : "Allow",
      "Action" : "pi:GetDimensionKeyDetails",
      "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsGetResourceMetadata",
      "Effect" : "Allow",
      "Action" : "pi:GetResourceMetadata",
      "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsGetResourceMetrics",
      "Effect" : "Allow",
```

```
      "Action" : "pi:GetResourceMetrics",
      "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsListAvailableResourceDimensions",
      "Effect" : "Allow",
      "Action" : "pi:ListAvailableResourceDimensions",
      "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsListAvailableResourceMetrics",
      "Effect" : "Allow",
      "Action" : "pi:ListAvailableResourceMetrics",
      "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsGetPerformanceAnalysisReport",
      "Effect" : "Allow",
      "Action" : "pi:GetPerformanceAnalysisReport",
      "Resource" : "arn:aws:pi:*:*:perf-reports/rds/*/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsListPerformanceAnalysisReports",
      "Effect" : "Allow",
      "Action" : "pi:ListPerformanceAnalysisReports",
      "Resource" : "arn:aws:pi:*:*:perf-reports/rds/*/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsListTagsForResource",
      "Effect" : "Allow",
      "Action" : "pi:ListTagsForResource",
      "Resource" : "arn:aws:pi:*:*:*/rds/*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonRDSPreviewServiceRolePolicy

説明: Amazon RDS Preview サービスロールポリシー

AmazonRDSPreviewServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 5 月 31 日 18:02 UTC
- 編集日時: 2024 年 8 月 7 日 01:02 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonRDSPreviewServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v9 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AssociateAddress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateCoipPoolPermission",
        "ec2:CreateLocalGatewayRouteTablePermission",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteCoipPoolPermission",
        "ec2:DeleteLocalGatewayRouteTablePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCoipPools",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLocalGatewayRouteTablePermissions",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeLocalGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:DisassociateAddress",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ReleaseAddress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/rds/*"
      ]
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/rds/*:log-stream:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/DocDB-Preview",
            "AWS/Neptune-Preview",
            "AWS/RDS-Preview",
            "AWS/Usage"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetRandomPassword"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:PutSecretValue",
        "secretsmanager:RotateSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:UpdateSecretVersionStage",
        "secretsmanager:ListSecretVersionIds"
      ],
```

```
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:rds-preview-us-east-2!*"
      ],
      "Condition" : {
        "StringLike" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "rds-preview-
us-east-2"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "secretsmanager:TagResource",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:rds-preview-us-east-2!*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws:rds:primaryDBInstanceArn",
            "aws:rds:primaryDBClusterArn"
          ]
        },
        "StringLike" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "rds-preview-
us-east-2"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonRDSReadOnlyAccess

説明: 経由で Amazon RDS への読み取り専用アクセスを提供します AWS マネジメントコンソール。

AmazonRDSReadOnlyAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRDSReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2023 年 4 月 14 日 12:32 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRDSReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonRDSServiceRolePolicy

説明: Amazon RDS がユーザーに代わって AWS リソースを管理できるようにします。

AmazonRDSServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 1 月 8 日 18:17 UTC
- 編集日時: 2024 年 7 月 01 日 22:42 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonRDSServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v14 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
    {
      "Sid" : "Ec2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AssociateAddress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateCoipPoolPermission",
        "ec2:CreateLocalGatewayRouteTablePermission",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteCoipPoolPermission",
        "ec2:DeleteLocalGatewayRouteTablePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCoipPools",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLocalGatewayRouteTablePermissions",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeLocalGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:DisassociateAddress",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifyVpcEndpoint",
        "ec2:ReleaseAddress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeVpcEndpoints",
        "ec2:DeleteVpcEndpoints",
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchLogs",
      "Effect" : "Allow",
      "Action" : [
```

```
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/rds/*",
        "arn:aws:logs:*:*:log-group:/aws/docdb/*",
        "arn:aws:logs:*:*:log-group:/aws/neptune/*"
      ]
    },
    {
      "Sid" : "CloudWatchStreams",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/rds/*:log-stream:*",
        "arn:aws:logs:*:*:log-group:/aws/docdb/*:log-stream:*",
        "arn:aws:logs:*:*:log-group:/aws/neptune/*:log-stream:*"
      ]
    },
    {
      "Sid" : "Kinesis",
      "Effect" : "Allow",
      "Action" : [
        "kinesis:CreateStream",
        "kinesis:PutRecord",
        "kinesis:PutRecords",
        "kinesis:DescribeStream",
        "kinesis:SplitShard",
        "kinesis:MergeShards",
        "kinesis:DeleteStream",
        "kinesis:UpdateShardCount"
      ],
      "Resource" : [
        "arn:aws:kinesis:*:*:stream/aws-rds-das-*"
      ]
    },
    {
      "Sid" : "CloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/DocDB",
            "AWS/Neptune",
            "AWS/RDS",
            "AWS/Usage"
          ]
        }
      }
    },
    {
      "Sid" : "SecretsManagerPassword",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetRandomPassword"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:PutSecretValue",
        "secretsmanager:RotateSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:UpdateSecretVersionStage",
        "secretsmanager:ListSecretVersionIds"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:rds!*"
      ],
      "Condition" : {
        "StringLike" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "rds"
        }
      }
    },
    {
      "Sid" : "SecretsManagerTags",
```

```
      "Effect" : "Allow",
      "Action" : "secretsmanager:TagResource",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:rds!*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws:rds:primaryDBInstanceArn",
            "aws:rds:primaryDBClusterArn"
          ]
        },
        "StringLike" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "rds"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonRedshiftAllCommandsFullAccess

説明: このポリシーには、Amazon Redshift のデータをコピー、ロード、アンロード、クエリ、分析するための SQL コマンドを実行するアクセス許可が含まれています。このポリシーは、Amazon S3、Amazon CloudWatch logs、Amazon SageMaker、Glue などの関連サービスの Select ステートメントを実行するアクセス許可も付与 AWS します。

`AmazonRedshiftAllCommandsFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonRedshiftAllCommandsFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2021 年 11 月 4 日 00:48 UTC
- 編集日時: 2021 年 11 月 25 日 02:27 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRedshiftAllCommandsFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonRedshiftDataFullAccess

説明: このポリシーは、Amazon Redshift Data API へのフルアクセスを提供します。このポリシーは、その他の必要なサービスへのスコープ付きアクセスも付与します。

`AmazonRedshiftDataFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonRedshiftDataFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 9 月 9 日 19:23 UTC
- 編集日時: 2023 年 4 月 7 日 18:18 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftDataFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonRedshiftFederatedAuthorization

説明: これは、Amazon Redshift フェデレーティッド認可でクエリを実行するためのease-of-useポリシーです。

AmazonRedshiftFederatedAuthorization は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRedshiftFederatedAuthorization をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 11 月 22 日 00:04 UTC

- 編集日時: 2025 年 11 月 22 日 00:04 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRedshiftFederatedAuthorization

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRedshiftFederatedAuthorization",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetCatalog",
        "glue:GetCatalogs",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetUserDefinedFunctions",
        "glue:CreateDatabase",
        "glue:CreateTable",
        "glue:DeleteDatabase",
        "glue:DeleteTable",
        "glue:UpdateCatalog",
        "glue:UpdateDatabase",
        "glue:UpdateTable",
        "glue:RenameTable",
        "glue:FederateAuthorization"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "glue:FederatedAuthorizationSource" : "Redshift"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftIdentityCenterSetContext",
      "Effect" : "Allow",
      "Action" : [
        "sts:SetContext"
      ],
      "Resource" : "arn:aws:sts::*:self"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonRedshiftFullAccess

説明: 経由で Amazon Redshift へのフルアクセスを提供します AWS マネジメントコンソール。

`AmazonRedshiftFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonRedshiftFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2022 年 7 月 7 日 23:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonRedshiftQueryEditor

説明: Amazon Redshift クエリエディタへのフルアクセスと、 AWS マネジメントコンソール経由で保存されたクエリへのフルアクセスを提供します。

`AmazonRedshiftQueryEditor` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonRedshiftQueryEditor` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 10 月 4 日 22:50 UTC
- 編集日時: 2021 年 2 月 16 日 19:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditor`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonRedshiftQueryEditorV2FullAccess

説明: Amazon Redshift Query Editor V2 のオペレーションとリソースに対する、フルアクセス権を付与します。このポリシーは、その他の必要なサービスへのアクセス権限も付与します。これには、Amazon Redshift クラスターの一覧表示、 AWS KMS でのキーとエイリアスの読み取り、 AWS Secrets Manager でのクエリエディタ V2 シークレットの管理のためのアクセス許可が含まれます。

`AmazonRedshiftQueryEditorV2FullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonRedshiftQueryEditorV2FullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 9 月 24 日 14:06 UTC
- 編集日時: 2024 年 2 月 21 日 17:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2FullAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonRedshiftQueryEditorV2NoSharing

説明: リソースを共有せずに Amazon Redshift Query Editor V2 を操作できる機能を付与します。権限を与えられたプリンシパルは、そのリソースの読み取り、更新、削除のみが可能で、共有はできません。このポリシーは、その他の必要なサービスへのアクセス権限も付与します。これには、Amazon Redshift クラスターを一覧表示し、 AWS Secrets Manager のプリンシパルのクエリエディタ V2 シークレットを管理するアクセス許可が含まれます。

`AmazonRedshiftQueryEditorV2NoSharing` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonRedshiftQueryEditorV2NoSharing` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2021 年 9 月 24 日 14:18 UTC
- 編集日時: 2024 年 2 月 21 日 17:25 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2NoSharing

ポリシーのバージョン

ポリシーのバージョン: v9 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonRedshiftQueryEditorV2ReadSharing

説明: 限定されたリソースを共有しながら、Amazon Redshift Query Editor V2 を操作できる機能を付与します。付与されたプリンシパルは、そのリソースを読み取り、書き込み、共有することができます。付与されたプリンシパルは、チームと共有されているリソースの読み取りはできますが、更新はできません。このポリシーは、その他の必要なサービスへのアクセス権限も付与します。これには、Amazon Redshift クラスターを一覧表示し、 AWS Secrets Manager のプリンシパルのクエリエディタ V2 シークレットを管理するアクセス許可が含まれます。

`AmazonRedshiftQueryEditorV2ReadSharing` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonRedshiftQueryEditorV2ReadSharing` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 9 月 24 日 14:22 UTC
- 編集日時: 2024 年 2 月 21 日 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2ReadSharing`

ポリシーのバージョン

ポリシーのバージョン: v9 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonRedshiftQueryEditorV2ReadWriteSharing

説明: リソースを共有しながら Amazon Redshift Query Editor V2 を操作する機能を付与します。付与されたプリンシパルは、そのリソースを読み取り、書き込み、共有することができます。付与されたプリンシパルは、そのチームと共有されているリソースを読み取り、更新することができます。このポリシーは、その他の必要なサービスへのアクセス権限も付与します。これには、Amazon Redshift クラスターを一覧表示し、 AWS Secrets Manager のプリンシパルのクエリエディタ V2 シークレットを管理するアクセス許可が含まれます。

AmazonRedshiftQueryEditorV2ReadWriteSharing は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRedshiftQueryEditorV2ReadWriteSharing をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 9 月 24 日 14:25 UTC
- 編集日時: 2024 年 2 月 21 日 17:30 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2ReadWriteSharing

ポリシーのバージョン

ポリシーのバージョン: v9 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonRedshiftReadOnlyAccess

説明: 経由で Amazon Redshift への読み取り専用アクセスを提供します AWS マネジメントコンソール。

AmazonRedshiftReadOnlyAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRedshiftReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2024 年 2 月 8 日 00:24 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRedshiftReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonRedshiftServiceLinkedRolePolicy

説明: Amazon Redshift がユーザーに代わって AWS サービスを呼び出すことを許可する

AmazonRedshiftServiceLinkedRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 9 月 18 日 19:19 UTC

- 編集日時: 2025 年 2 月 19 日 17:22 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonRedshiftServiceLinkedRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v15 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Ec2VpcPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAddresses",
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:CreateVpcEndpoint",
        "ec2:DeleteVpcEndpoints",
        "ec2:DescribeVpcEndpoints",
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PublicAccessCreateEip",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:AllocateAddress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:elastic-ip/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/Redshift" : "true"
        }
      }
    },
    {
      "Sid" : "PublicAccessReleaseEip",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ReleaseAddress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:elastic-ip/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/Redshift" : "true"
        }
      }
    },
    {
      "Sid" : "EnableCreationAndManagementOfRedshiftCloudwatchLogGroups",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/redshift/*"
      ]
    },
    {
      "Sid" : "EnableCreationAndManagementOfRedshiftCloudwatchLogStreams",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams",
```

```
        "logs:GetLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/redshift/*:log-stream:*"
      ]
    },
    {
      "Sid" : "CreateSecurityGroupWithTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/Redshift" : "true"
        }
      }
    },
    {
      "Sid" : "SecurityGroupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:ModifySecurityGroupRules",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/Redshift" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSecurityGroup",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "CreateTagsOnResources",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:internet-gateway/*",
        "arn:aws:ec2:*:*:elastic-ip/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateVpc",
            "CreateSecurityGroup",
            "CreateSubnet",
            "CreateInternetGateway",
            "CreateRouteTable",
            "AllocateAddress"
          ]
        }
      }
    },
    {
      "Sid" : "VPCPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeRouteTables"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/Redshift-Serverless",
            "AWS/Redshift"
          ]
        }
      }
    },
    {
      "Sid" : "SecretManager",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:PutSecretValue",
        "secretsmanager:UpdateSecret",
        "secretsmanager:UpdateSecretVersionStage",
        "secretsmanager:RotateSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:redshift!*"
      ],
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "redshift",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SecretsManagerRandomPassword",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetRandomPassword"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IPV6Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignIpv6Addresses",
        "ec2:UnassignIpv6Addresses"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    },
    {
      "Sid" : "ServiceQuotasToCheckCustomerLimits",
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : [
        "arn:aws:servicequotas:*:*:ec2/L-0263D0A3",
        "arn:aws:servicequotas:*:*:vpc/L-29B6F2EB"
      ]
    },
    {
      "Sid" : "DiscoverRedshiftCatalogs",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetCatalog",
        "glue:GetCatalogs"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*"
      ],
      "Condition" : {
        "Bool" : {
          "glue:EnabledForRedshiftAutoDiscovery" : "true"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Sid" : "LakeFormationGetMetadataAccessForFederatedCatalogs",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataAccess"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "Bool" : {
          "lakeformation:EnabledOnlyForMetaDataAccess" : "true"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "glue.amazonaws.com"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonRekognitionCustomLabelsFullAccess

説明: このポリシーは、Amazon Rekognition Custom Labels 機能に必要な rekognition および S3 アクセス許可を指定します。

`AmazonRekognitionCustomLabelsFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonRekognitionCustomLabelsFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 1 月 8 日 19:18 UTC
- 編集日時: 2022 年 8 月 16 日 20:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRekognitionCustomLabelsFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonRekognitionFullAccess

説明: すべての Amazon Rekognition API へのアクセス

`AmazonRekognitionFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRekognitionFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2016 年 11 月 30 日 14:40 UTC
- 編集日時: 2016 年 11 月 30 日 14:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRekognitionFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonRekognitionReadOnlyAccess

説明: すべての読み取り rekognition API へのアクセス

AmazonRekognitionReadOnlyAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRekognitionReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2016 年 11 月 30 日 14:58 UTC
- 編集日時: 2023 年 11 月 8 日 18:30 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRekognitionReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v10 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonRekognitionServiceRole

説明: Rekognition がユーザーに代わって AWS サービスを呼び出すことを許可します。

AmazonRekognitionServiceRole は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRekognitionServiceRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2017 年 11 月 29 日 16:52 UTC
- 編集日時: 2017 年 11 月 29 日 16:52 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonRekognitionServiceRole

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonRoute53AutoNamingFullAccess

説明: Route 53 のすべての自動命名アクションへのフルアクセスを提供します。

AmazonRoute53AutoNamingFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRoute53AutoNamingFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 1 月 18 日 18:40 UTC
- 編集日時: 2018 年 1 月 18 日 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53AutoNamingFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonRoute53AutoNamingReadOnlyAccess

説明: Route 53 のすべての自動命名アクションへの読み取り専用アクセスを提供します。

`AmazonRoute53AutoNamingReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonRoute53AutoNamingReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 1 月 18 日 03:02 UTC
- 編集日時: 2018 年 1 月 18 日 03:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53AutoNamingReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonRoute53AutoNamingRegistrantAccess

説明: Route 53 自動命名アクションへの登録者レベルのアクセスを提供します。

AmazonRoute53AutoNamingRegistrantAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRoute53AutoNamingRegistrantAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2018 年 3 月 12 日 22:33 UTC
- 編集日時: 2018 年 3 月 12 日 22:33 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53AutoNamingRegistrantAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonRoute53DomainsFullAccess

説明: Route53 Domains のすべてのアクションへのフルアクセスを提供し、ドメイン登録の一環としてホストゾーンを作成できるようにします。

`AmazonRoute53DomainsFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonRoute53DomainsFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2015 年 2 月 6 日 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53DomainsFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:CreateHostedZone",
        "route53domains:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonRoute53DomainsReadOnlyAccess

説明: Route53 ドメインのリストとアクションへのアクセスを提供します。

AmazonRoute53DomainsReadOnlyAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRoute53DomainsReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2015 年 2 月 6 日 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53DomainsReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53domains:Get*",
        "route53domains:List*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonRoute53FullAccess

説明: AWS マネジメントコンソールを介してすべての Amazon Route 53 へのフルアクセスを提供します。

AmazonRoute53FullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRoute53FullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2025 年 5 月 15 日 18:07 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53FullAccess

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:*",
        "route53domains:*",
        "cloudfront:ListDistributions",
        "cloudfront:GetDistributionTenantByDomain",
        "cloudfront:GetConnectionGroup",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:GetMetricData",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeRegions",
        "elasticloadbalancing:DescribeLoadBalancers",
```

```
        "elasticbeanstalk:DescribeEnvironments",
        "es:ListDomainNames",
        "es:DescribeDomains",
        "lightsail:GetContainerServices",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:GetBucketWebsite",
        "sns:ListTopics",
        "sns:ListSubscriptionsByTopic",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "apigateway:GET",
      "Resource" : "arn:aws:apigateway:*::/domainnames"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonRoute53ProfilesFullAccess

説明: このポリシーは Amazon Route 53 Profile リソースへのフルアクセスを許可します。

AmazonRoute53ProfilesFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRoute53ProfilesFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 4 月 30 日 18:30 UTC
- 編集日時: 2024 年 8 月 27 日 19:18 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ProfilesFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRoute53ProfilesFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "route53profiles:AssociateProfile",
        "route53profiles:AssociateResourceToProfile",
        "route53profiles:CreateProfile",
        "route53profiles:DeleteProfile",
        "route53profiles:DisassociateProfile",
        "route53profiles:DisassociateResourceFromProfile",
        "route53profiles:GetProfile",
        "route53profiles:GetProfileAssociation",
        "route53profiles:GetProfilePolicy",
        "route53profiles:GetProfileResourceAssociation",
        "route53profiles:ListProfileAssociations",
        "route53profiles:ListProfileResourceAssociations",
        "route53profiles:ListProfiles",
        "route53profiles:ListTagsForResource",
        "route53profiles:PutProfilePolicy",
        "route53profiles:TagResource",
```

```
        "route53profiles:UntagResource",
        "route53profiles:UpdateProfileResourceAssociation",
        "route53resolver:GetFirewallConfig",
        "route53resolver:GetFirewallRuleGroup",
        "route53resolver:GetResolverConfig",
        "route53resolver:GetResolverDnssecConfig",
        "route53resolver:GetResolverQueryLogConfig",
        "route53resolver:GetResolverRule",
        "ec2:DescribeVpcs",
        "route53:GetHostedZone"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonRoute53ProfilesReadOnlyAccess

説明: このポリシーは、Amazon Route 53 Profile リソースへの読み取り専用アクセスを許可します。

`AmazonRoute53ProfilesReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonRoute53ProfilesReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2024 年 4 月 30 日 18:29 UTC
- 編集日時: 2024 年 8 月 27 日 18:59 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53ProfilesReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRoute53ProfilesReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "route53profiles:GetProfile",
        "route53profiles:GetProfileAssociation",
        "route53profiles:GetProfilePolicy",
        "route53profiles:GetProfileResourceAssociation",
        "route53profiles:ListProfileAssociations",
        "route53profiles:ListProfileResourceAssociations",
        "route53profiles:ListProfiles",
        "route53profiles:ListTagsForResource",
        "route53resolver:GetFirewallConfig",
        "route53resolver:GetResolverConfig",
        "route53resolver:GetResolverDnssecConfig",
        "route53resolver:GetResolverQueryLogConfig"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonRoute53ReadOnlyAccess

説明: AWS マネジメントコンソールを介してすべての Amazon Route 53 への読み取り専用アクセスを提供します。

`AmazonRoute53ReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonRoute53ReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2016 年 11 月 15 日 21:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:Get*",
        "route53:List*",
        "route53:TestDNSAnswer"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonRoute53RecoveryClusterFullAccess

説明: Amazon Route 53 Recovery クラスター へのフルアクセスを提供します

`AmazonRoute53RecoveryClusterFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonRoute53RecoveryClusterFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 8 月 18 日 18:37 UTC

- 編集日時: 2021 年 8 月 18 日 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryClusterFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-cluster:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonRoute53RecoveryClusterReadOnlyAccess

説明: Amazon Route 53 リカバリクラスターへの読み取り専用アクセスを提供します

`AmazonRoute53RecoveryClusterReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRoute53RecoveryClusterReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 8 月 18 日 17:36 UTC
- 編集日時: 2022 年 4 月 1 日 17:37 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53RecoveryClusterReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-cluster:GetRoutingControlState",
        "route53-recovery-cluster:ListRoutingControls"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する

- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonRoute53RecoveryControlConfigFullAccess

説明: Amazon Route 53 リカバリコントロール 設定へのフルアクセスを提供します

AmazonRoute53RecoveryControlConfigFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRoute53RecoveryControlConfigFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 8 月 18 日 17:48 UTC
- 編集日時: 2021 年 8 月 18 日 17:48 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53RecoveryControlConfigFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
      "Action" : [
        "route53-recovery-control-config:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonRoute53RecoveryControlConfigReadOnlyAccess

説明: Amazon Route 53 リカバリコントロール設定への読み取り専用アクセスを提供します

`AmazonRoute53RecoveryControlConfigReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonRoute53RecoveryControlConfigReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 8 月 18 日 18:01 UTC
- 編集日時: 2023 年 10 月 18 日 17:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryControlConfigReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonRoute53RecoveryReadinessFullAccess

説明: Amazon Route 53 リカバリ対応機能へのフルアクセスを提供します

AmazonRoute53RecoveryReadinessFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRoute53RecoveryReadinessFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 8 月 18 日 16:45 UTC
- 編集日時: 2021 年 8 月 18 日 16:45 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53RecoveryReadinessFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-readiness:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonRoute53RecoveryReadinessReadOnlyAccess

説明: は、Amazon Route 53 のリカバリ対応機能への読み取り専用アクセスを提供します

`AmazonRoute53RecoveryReadinessReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonRoute53RecoveryReadinessReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 8 月 18 日 18:11 UTC
- 編集日時: 2021 年 11 月 9 日 20:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryReadinessReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
```

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonRoute53ResolverFullAccess

説明: Route 53 Resolver のフルアクセスポリシー

AmazonRoute53ResolverFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRoute53ResolverFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 5 月 30 日 18:10 UTC
- 編集日時: 2024 年 8 月 5 日 20:06 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53ResolverFullAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRoute53ResolverFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:*",
        "ec2:DescribeSubnets",
        "ec2:CreateNetworkInterface",
```

```
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfaces",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeAavailabilityZones"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonRoute53ResolverReadOnlyAccess

説明: Route 53 Resolver の読み取り専用ポリシー

`AmazonRoute53ResolverReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonRoute53ResolverReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 5 月 30 日 18:11 UTC
- 編集日時: 2024 年 8 月 5 日 18:54 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ResolverReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRoute53ResolverReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:Get*",
        "route53resolver:List*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonS3FullAccess

説明: 経由ですべてのバケットへのフルアクセスを提供します AWS マネジメントコンソール。

AmazonS3FullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonS3FullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2021 年 9 月 27 日 20:16 UTC
- ARN: arn:aws:iam::aws:policy/AmazonS3FullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:*",
        "s3-object-lambda:*"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonS3ObjectLambdaExecutionRolePolicy

説明: Amazon S3 Object AWS Lambda を操作するための Lambda 関数のアクセス許可を提供します。また、Amazon CloudWatch Logs に書き込むアクセス許可を Lambda に付与します。

`AmazonS3ObjectLambdaExecutionRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonS3ObjectLambdaExecutionRolePolicy` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2021 年 8 月 18 日 10:07 UTC
- 編集日時: 2021 年 8 月 18 日 10:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonS3ObjectLambdaExecutionRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "s3-object-lambda:WriteGetObjectResponse"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonS3OutpostsFullAccess

説明: 経由で Amazon S3 on Outposts へのフルアクセスを提供します AWS マネジメントコンソール。

`AmazonS3OutpostsFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonS3OutpostsFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2020 年 10 月 2 日 17:26 UTC
- 編集日時: 2020 年 10 月 2 日 17:26 UTC
- ARN: arn:aws:iam::aws:policy/AmazonS3OutpostsFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonS3OutpostsReadOnlyAccess

説明: 経由で Amazon S3 on Outposts への読み取り専用アクセスを提供します AWS マネジメントコンソール。

`AmazonS3OutpostsReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonS3OutpostsReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 10 月 2 日 18:55 UTC
- 編集日時: 2020 年 10 月 2 日 18:55 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3OutpostsReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonS3ReadOnlyAccess

説明: を介してすべてのバケットへの読み取り専用アクセスを提供します AWS マネジメントコンソール。

`AmazonS3ReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonS3ReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2023 年 8 月 10 日 21:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:Get*",
        "s3:List*",
        "s3:Describe*",
        "s3-object-lambda:Get*",
        "s3-object-lambda:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonS3TablesFullAccess

説明: すべての S3 テーブルバケットへのフルアクセスを提供します。

`AmazonS3TablesFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonS3TablesFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 12 月 3 日 15:21 UTC
- 編集日時: 2025 年 12 月 2 日 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3TablesFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3tables:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassRoleToS3TablesReplication",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "replication.s3tables.amazonaws.com"
          ]
        }
```

```
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonS3TablesLakeFormationServiceRole

説明: この管理ポリシーは、アカウント内のすべてのテーブルバケット、名前空間、およびテーブルを操作するアクセス許可を AWS Lake Formation に付与します。

`AmazonS3TablesLakeFormationServiceRole` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonS3TablesLakeFormationServiceRole` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2025 年 6 月 19 日 19:07 UTC
- 編集日時: 2025 年 7 月 9 日 22:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonS3TablesLakeFormationServiceRole`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PermissionsForS3ListTableBuckets",
      "Effect" : "Allow",
      "Action" : [
        "s3tables:ListTableBuckets"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DataAccessPermissionsForS3TablesResources",
      "Effect" : "Allow",
      "Action" : [
        "s3tables:CreateTableBucket",
        "s3tables:GetTableBucket",
        "s3tables:CreateNamespace",
        "s3tables:GetNamespace",
        "s3tables:ListNamespaces",
        "s3tables:DeleteNamespace",
        "s3tables:DeleteTableBucket",
        "s3tables:CreateTable",
        "s3tables:DeleteTable",
        "s3tables:GetTable",
        "s3tables:ListTables",
        "s3tables:RenameTable",
        "s3tables:UpdateTableMetadataLocation",
        "s3tables:GetTableMetadataLocation",
        "s3tables:GetTableData",
```

```
        "s3tables:PutTableData",
        "s3tables:PutTableBucketEncryption"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "KMSDataAccessPermissionsForS3TablesResources",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "s3.*.amazonaws.com"
          ],
          "kms:EncryptionContext:aws:s3:arn" : "arn:aws:s3tables:*:*:bucket/*/table/*"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "KMSDescribeKeyAccessPermissionsForS3TablesResources",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "s3tables.*.amazonaws.com"
          ]
```

```
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonS3TablesReadOnlyAccess

説明: すべての S3 テーブルバケットへの読み取り専用アクセスを提供します。

`AmazonS3TablesReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonS3TablesReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 12 月 3 日 15:21 UTC
- 編集日時: 2024 年 12 月 3 日 15:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3TablesReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3tables:Get*",
        "s3tables:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy

説明: Amazon SageMaker 製品ポートフォリオから製品をプロビジョニングするために AWS のサービス Catalog サービスで使用されるサービスロールポリシー。 Amazon SageMaker CodePipeline、CodeBuild、CodeCommit、Glue、CloudFormation などの一連の関連サービスにアクセス許可を付与します。

`AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 11 月 27 日 18:48 UTC
- 編集日時: 2025 年 9 月 27 日 04:34 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v10 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonSageMakerServiceCatalogAPIGatewayPermission",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET",
        "apigateway:POST",
        "apigateway:PUT",
        "apigateway:PATCH",
        "apigateway:DELETE"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/sagemaker:launch-source" : "*"
```

```
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogAPIGatewayPostPermission",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:POST"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "sagemaker:launch-source"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogAPIGatewayPatchPermission",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:PATCH"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/account"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCFnMutatePermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack",
        "cloudformation:DeleteStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/SC-*",
      "Condition" : {
        "ArnLikeIfExists" : {
          "cloudformation:RoleArn" : [
            "arn:aws:sts::*:assumed-role/AmazonSageMakerServiceCatalog*"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCFnTagPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/SC-*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:project-name" : "false"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCFnReadPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/SC-*"
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCFnTemplatePermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:GetTemplateSummary",
        "cloudformation:ValidateTemplate"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCodeBuildPermission",
      "Effect" : "Allow",
      "Action" : [
        "codebuild:CreateProject",
        "codebuild:DeleteProject",
        "codebuild:UpdateProject"
      ],
      "Resource" : [
        "arn:aws:codebuild:*:*:project/sagemaker-*"
      ]
```

```
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCodeCommitPermission",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:CreateCommit",
        "codecommit:CreateRepository",
        "codecommit:DeleteRepository",
        "codecommit:GetRepository",
        "codecommit:TagResource"
      ],
      "Resource" : [
        "arn:aws:codecommit:*:*:sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCodeCommitListPermission",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:ListRepositories"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCodePipelinePermission",
      "Effect" : "Allow",
      "Action" : [
        "codepipeline:CreatePipeline",
        "codepipeline:DeletePipeline",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:StartPipelineExecution",
        "codepipeline:TagResource",
        "codepipeline:UpdatePipeline"
      ],
      "Resource" : [
        "arn:aws:codepipeline:*:*:sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCIAMUserPermission",
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:CreateUserPool",
```

```
        "cognito-idp:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "sagemaker:launch-source"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCIAMPermission",
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:CreateGroup",
        "cognito-idp:CreateUserPoolDomain",
        "cognito-idp:CreateUserPoolClient",
        "cognito-idp:DeleteGroup",
        "cognito-idp:DeleteUserPool",
        "cognito-idp:DeleteUserPoolClient",
        "cognito-idp:DeleteUserPoolDomain",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:UpdateUserPool",
        "cognito-idp:UpdateUserPoolClient"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/sagemaker:launch-source" : "*"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogECRPermission",
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository",
        "ecr:DeleteRepository",
        "ecr:TagResource"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/sagemaker-*"
```

```
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogEventBridgePermission",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:DeleteRule",
        "events:DisableRule",
        "events:EnableRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogFirehosePermission",
      "Effect" : "Allow",
      "Action" : [
        "firehose:CreateDeliveryStream",
        "firehose:DeleteDeliveryStream",
        "firehose:DescribeDeliveryStream",
        "firehose:StartDeliveryStreamEncryption",
        "firehose:StopDeliveryStreamEncryption",
        "firehose:UpdateDestination"
      ],
      "Resource" : "arn:aws:firehose:*:*:deliverystream/sagemaker-*"
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogGluePermission",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:DeleteDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/sagemaker-*",
        "arn:aws:glue:*:*:table/sagemaker-*",
        "arn:aws:glue:*:*:userDefinedFunction/sagemaker-*"
      ]
```

```
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogGlueClassiferPermission",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateClassifier",
        "glue:DeleteClassifier",
        "glue:DeleteCrawler",
        "glue:DeleteJob",
        "glue:DeleteTrigger",
        "glue:DeleteWorkflow",
        "glue:StopCrawler"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogGlueWorkflowPermission",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateWorkflow"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:workflow/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogGlueJobPermission",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateJob"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:job/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogGlueCrawlerPermission",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateCrawler",
        "glue:GetCrawler"
      ],
```

```
      "Resource" : [
        "arn:aws:glue:*:*:crawler/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogGlueTriggerPermission",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateTrigger",
        "glue:GetTrigger"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:trigger/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogPassRolePermission",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSageMakerServiceCatalog*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogLambdaPermission",
      "Effect" : "Allow",
      "Action" : [
        "lambda:AddPermission",
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:InvokeFunction",
        "lambda:RemovePermission"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogLambdaTagPermission",
      "Effect" : "Allow",
```

```
      "Action" : "lambda:TagResource",
      "Resource" : [
        "arn:aws:lambda:*:*:function:sagemaker-*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "sagemaker:*"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogLogGroupPermission",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DeleteLogGroup",
        "logs:DeleteLogStream",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/apigateway/AccessLogs/*",
        "arn:aws:logs:*:*:log-group::log-stream:*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogS3ReadPermission",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "s3:ExistingObjectTag/servicecatalog:provisioning" : "true"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogS3ReadSagemakerResourcePermission",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
```

```
      "Resource" : [
        "arn:aws:s3:::sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogS3MutatePermission",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteBucketPolicy",
        "s3:GetBucketPolicy",
        "s3:PutBucketAcl",
        "s3:PutBucketNotification",
        "s3:PutBucketPolicy",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketLogging",
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketCORS",
        "s3:PutBucketTagging",
        "s3:PutObjectTagging"
      ],
      "Resource" : "arn:aws:s3:::sagemaker-*"
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogSageMakerPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateModel",
        "sagemaker:CreateWorkteam",
        "sagemaker:DeleteEndpoint",
        "sagemaker:DeleteEndpointConfig",
        "sagemaker:DeleteModel",
        "sagemaker:DeleteWorkteam",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeWorkteam",
        "sagemaker:CreateCodeRepository",
        "sagemaker:DescribeCodeRepository",
        "sagemaker:UpdateCodeRepository",
        "sagemaker:DeleteCodeRepository"
```

```
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogSageMakerTagPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:model/*",
        "arn:aws:sagemaker:*:*:pipeline/*",
        "arn:aws:sagemaker:*:*:project/*",
        "arn:aws:sagemaker:*:*:model-package/*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "sagemaker:*"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogSageMakerImagePermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateImage",
        "sagemaker:DeleteImage",
        "sagemaker:DescribeImage",
        "sagemaker:UpdateImage",
        "sagemaker:ListTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:image/*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogStepFunctionPermission",
      "Effect" : "Allow",
```

```
      "Action" : [
        "states:CreateStateMachine",
        "states:DeleteStateMachine",
        "states:UpdateStateMachine"
      ],
      "Resource" : [
        "arn:aws:states:*:*:stateMachine:sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCodeStarPermission",
      "Effect" : "Allow",
      "Action" : "codestar-connections:PassConnection",
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "codestar-connections:PassedToService" : "codepipeline.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCodeConnectionPermission",
      "Effect" : "Allow",
      "Action" : "codeconnections:PassConnection",
      "Resource" : [
        "arn:aws:codeconnections:*:*:connection/*",
        "arn:aws:codestar-connections:*:*:connection/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "codeconnections:PassedToService" : "codepipeline.amazonaws.com"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する

- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonSageMakerCanvasAIServicesAccess

説明: Amazon SageMaker Canvas に、AI サービスを使用してすぐに利用可能な AI ソリューションをサポートするためのアクセス許可を提供します。このポリシーでは、Amazon SageMaker Canvas がサポートを追加するにつれて、サービスに対する変更権限がさらに追加されます。

AmazonSageMakerCanvasAIServicesAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerCanvasAIServicesAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 3 月 23 日 22:36 UTC
- 編集日時: 2023 年 11 月 29 日 14:47 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerCanvasAIServicesAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonSageMakerCanvasBedrockAccess

説明: このポリシーでは、S3 などの下流サービスへのアクセスにより SageMaker Canvas で Amazon Bedrock を使用するアクセス許可を付与します。

AmazonSageMakerCanvasBedrockAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerCanvasBedrockAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 2 月 2 日 18:37 UTC
- 編集日時: 2024 年 2 月 2 日 18:37 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerCanvasBedrockAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonSageMakerCanvasDataPrepFullAccess

説明: Canvas でのデータ準備のための Amazon SageMaker リソースとオペレーションへのフルアクセスを提供します。このポリシーでは、関連サービス (S3、IAM、KMS、RDS、CloudWatch Logs、Redshift、Athena、Glue、EventBridge、Secrets Manager など) への特定のアクセスも提供されます。このポリシーを、Amazon SageMaker ドメイン/ユーザープロファイル実行ロールにアタッチします。

`AmazonSageMakerCanvasDataPrepFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonSageMakerCanvasDataPrepFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 10 月 27 日 22:56 UTC
- 編集日時: 2024 年 8 月 16 日 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasDataPrepFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SageMakerListFeatureGroupOperation",
      "Effect" : "Allow",
      "Action" : "sagemaker:ListFeatureGroups",
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerFeatureGroupOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateFeatureGroup",
        "sagemaker:DescribeFeatureGroup"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:feature-group/*"
    },
    {
      "Sid" : "SageMakerProcessingJobOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateProcessingJob",
```

```
        "sagemaker:DescribeProcessingJob",
        "sagemaker:AddTags"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:processing-job/*canvas-data-prep*"
    },
    {
      "Sid" : "SageMakerProcessingJobListOperation",
      "Effect" : "Allow",
      "Action" : "sagemaker:ListProcessingJobs",
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerPipelineOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribePipeline",
        "sagemaker:CreatePipeline",
        "sagemaker:UpdatePipeline",
        "sagemaker:DeletePipeline",
        "sagemaker:StartPipelineExecution",
        "sagemaker:ListPipelineExecutionSteps",
        "sagemaker:DescribePipelineExecution"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:pipeline/*canvas-data-prep*"
    },
    {
      "Sid" : "KMSListOperations",
      "Effect" : "Allow",
      "Action" : "kms:ListAliases",
      "Resource" : "*"
    },
    {
      "Sid" : "KMSOperations",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
      "Sid" : "S3Operations",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
```

```
        "s3:GetBucketCors",
        "s3:GetBucketLocation",
        "s3:AbortMultipartUpload"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3GetObjectOperation",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/SageMaker" : "true"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3ListOperations",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMListOperations",
      "Effect" : "Allow",
      "Action" : "iam:ListRoles",
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "IAMGetOperations",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Sid" : "IAMPassOperation",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com",
            "events.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "EventBridgePutOperation",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-data-prep-job" : "true"
        }
      }
    },
    {
      "Sid" : "EventBridgeOperations",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:PutTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sagemaker:is-canvas-data-prep-job" : "true"
```

```
        }
      }
    },
    {
      "Sid" : "EventBridgeTagBasedOperations",
      "Effect" : "Allow",
      "Action" : [
        "events:TagResource"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-data-prep-job" : "true",
          "aws:ResourceTag/sagemaker:is-canvas-data-prep-job" : "true"
        }
      }
    },
    {
      "Sid" : "EventBridgeListTagOperation",
      "Effect" : "Allow",
      "Action" : "events:ListTagsForResource",
      "Resource" : "*"
    },
    {
      "Sid" : "GlueOperations",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:SearchTables"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*"
      ]
    },
    {
      "Sid" : "EMROperations",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:ListInstanceGroups"
```

```
      ],
      "Resource" : "arn:aws:elasticmapreduce:*:*:cluster/*"
    },
    {
      "Sid" : "EMRListOperation",
      "Effect" : "Allow",
      "Action" : "elasticmapreduce:ListClusters",
      "Resource" : "*"
    },
    {
      "Sid" : "AthenaListDataCatalogOperation",
      "Effect" : "Allow",
      "Action" : "athena:ListDataCatalogs",
      "Resource" : "*"
    },
    {
      "Sid" : "AthenaQueryExecutionOperations",
      "Effect" : "Allow",
      "Action" : [
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:StartQueryExecution",
        "athena:StopQueryExecution"
      ],
      "Resource" : "arn:aws:athena:*:*:workgroup/*"
    },
    {
      "Sid" : "AthenaDataCatalogOperations",
      "Effect" : "Allow",
      "Action" : [
        "athena:ListDatabases",
        "athena:ListTableMetadata"
      ],
      "Resource" : "arn:aws:athena:*:*:datacatalog/*"
    },
    {
      "Sid" : "RedshiftOperations",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:DescribeStatement",
        "redshift-data:CancelStatement",
        "redshift-data:GetStatementResult"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "RedshiftArnBasedOperations",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:ExecuteStatement",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables"
      ],
      "Resource" : "arn:aws:redshift:*:*:cluster:*"
    },
    {
      "Sid" : "RedshiftGetCredentialsOperation",
      "Effect" : "Allow",
      "Action" : "redshift:GetClusterCredentials",
      "Resource" : [
        "arn:aws:redshift:*:*:dbuser:*/sagemaker_access*",
        "arn:aws:redshift:*:*:dbname:*"
      ]
    },
    {
      "Sid" : "SecretsManagerARNBasedOperation",
      "Effect" : "Allow",
      "Action" : "secretsmanager:CreateSecret",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonSageMaker-*"
    },
    {
      "Sid" : "SecretManagerTagBasedOperation",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonSageMaker-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SageMaker" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RDSOperation",
      "Effect" : "Allow",
```

```
      "Action" : "rds:DescribeDBInstances",
      "Resource" : "*"
    },
    {
      "Sid" : "LoggingOperation",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/sagemaker/studio:*"
    },
    {
      "Sid" : "EMRServerlessCreateApplicationOperation",
      "Effect" : "Allow",
      "Action" : "emr-serverless:CreateApplication",
      "Resource" : "arn:aws:emr-serverless:*:*:/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessListApplicationOperation",
      "Effect" : "Allow",
      "Action" : "emr-serverless:ListApplications",
      "Resource" : "arn:aws:emr-serverless:*:*:/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessApplicationOperations",
      "Effect" : "Allow",
      "Action" : [
        "emr-serverless:UpdateApplication",
        "emr-serverless:GetApplication"
      ],
      "Resource" : "arn:aws:emr-serverless:*:*:/applications/*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessStartJobRunOperation",
      "Effect" : "Allow",
      "Action" : "emr-serverless:StartJobRun",
      "Resource" : "arn:aws:emr-serverless:*:*:/applications/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessListJobRunOperation",
      "Effect" : "Allow",
      "Action" : "emr-serverless:ListJobRuns",
      "Resource" : "arn:aws:emr-serverless:*:*:/applications/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessJobRunOperations",
      "Effect" : "Allow",
      "Action" : [
        "emr-serverless:GetJobRun",
        "emr-serverless:CancelJobRun"
      ],
      "Resource" : "arn:aws:emr-serverless:*:*:/applications/*/jobruns/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "EMRServerlessTagResourceOperation",
      "Effect" : "Allow",
      "Action" : "emr-serverless:TagResource",
      "Resource" : "arn:aws:emr-serverless:*:*:/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "IAMPassOperationForEMRServerless",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSageMakerCanvasEMRSExecutionAccess-*",
        "arn:aws:iam::*:role/AmazonSageMakerCanvasEMRSExecutionAccess-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "emr-serverless.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonSageMakerCanvasDirectDeployAccess

説明: Amazon SageMaker Canvas が Canvas を通じて作成されたエンドポイントのエンドポイント詳細を作成、管理、表示できるようにします。Amazon SageMaker Canvas が CloudWatch からエンドポイント呼び出しメトリクスを取得できるようにします。

`AmazonSageMakerCanvasDirectDeployAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonSageMakerCanvasDirectDeployAccess` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 10 月 6 日 18:11 UTC
- 編集日時: 2023 年 10 月 6 日 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerCanvasDirectDeployAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonSageMakerCanvasEMRServerlessExecutionRolePolicy

説明: このポリシーは、Amazon SageMaker Canvas が大規模なデータ処理に使用する S3 などのサービスに対するアクセス許可を Amazon EMR Serverless に付与します。

AmazonSageMakerCanvasEMRServerlessExecutionRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerCanvasEMRServerlessExecutionRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 7 月 27 日 00:35 UTC
- 編集日時: 2024 年 7 月 27 日 00:35 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasEMRServerlessExecutionRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "S3Operations",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:GetBucketCors",
        "s3:GetBucketLocation",
        "s3:AbortMultipartUpload"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*sagemaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "S3GetObjectOperation",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/SageMaker" : "true"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3ListOperations",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonSageMakerCanvasForecastAccess

説明: このポリシーは、Amazon Forecast で SageMaker Canvas を使用するために一般的に必要となるアクセス許可を付与します。

AmazonSageMakerCanvasForecastAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerCanvasForecastAccess をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 8 月 24 日 20:04 UTC
- 編集日時: 2022 年 8 月 24 日 20:04 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerCanvasForecastAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonSageMakerCanvasFullAccess

説明: Amazon SageMaker Canvas のリソースとオペレーションへのフルアクセスを提供します。このポリシーでは、関連サービス (S3、IAM、VPC、ECR、CloudWatch Logs、Redshift、Secrets Manager、Forecast など) への特定のアクセスも提供されます。このポリシーを、Amazon SageMaker ドメイン/ユーザープロファイル実行ロールにアタッチします。

`AmazonSageMakerCanvasFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonSageMakerCanvasFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 9 月 9 日 00:44 UTC
- 編集日時: 2024 年 8 月 16 日 04:35 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v11 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SageMakerUserDetailsAndPackageOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeUserProfile",
        "sagemaker:ListTags",
        "sagemaker:ListModelPackages",
        "sagemaker:ListModelPackageGroups",
        "sagemaker:ListEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerPackageGroupOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateModelPackageGroup",
        "sagemaker:CreateModelPackage",
        "sagemaker:DescribeModelPackageGroup",
```

```
        "sagemaker:DescribeModelPackage"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:model-package/*",
        "arn:aws:sagemaker:*:*:model-package-group/*"
      ]
    },
    {
      "Sid" : "SageMakerTrainingOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateCompilationJob",
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateModel",
        "sagemaker:CreateProcessingJob",
        "sagemaker:CreateAutoMLJob",
        "sagemaker:CreateAutoMLJobV2",
        "sagemaker:CreateTrainingJob",
        "sagemaker:CreateTransformJob",
        "sagemaker:DeleteEndpoint",
        "sagemaker:DescribeCompilationJob",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeAutoMLJob",
        "sagemaker:DescribeAutoMLJobV2",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:DescribeTransformJob",
        "sagemaker:ListCandidatesForAutoMLJob",
        "sagemaker:StopAutoMLJob",
        "sagemaker:StopTrainingJob",
        "sagemaker:StopTransformJob",
        "sagemaker:AddTags",
        "sagemaker:DeleteApp"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:*Canvas*",
        "arn:aws:sagemaker:*:*:*canvas*",
        "arn:aws:sagemaker:*:*:*model-compilation-*"
      ]
    },
    {
```

```
      "Sid" : "SageMakerHostingOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DeleteEndpointConfig",
        "sagemaker:DeleteModel",
        "sagemaker:InvokeEndpoint",
        "sagemaker:UpdateEndpointWeightsAndCapacities",
        "sagemaker:InvokeEndpointAsync"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:*Canvas*",
        "arn:aws:sagemaker:*:*:*canvas*"
      ]
    },
    {
      "Sid" : "EC2VPCOperation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServices"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ECROperations",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchGetImage",
        "ecr:GetDownloadUrlForLayer",
        "ecr:GetAuthorizationToken"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMGetOperations",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*"
```

```
    },
    {
      "Sid" : "IAMPassOperation",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "sagemaker.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "LoggingOperation",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/sagemaker/*"
    },
    {
      "Sid" : "S3Operations",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:CreateBucket",
        "s3:GetBucketCors",
        "s3:GetBucketLocation"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
      ]
    },
    {
      "Sid" : "ReadSageMakerJumpstartArtifacts",
      "Effect" : "Allow",
```

```
      "Action" : "s3:GetObject",
      "Resource" : [
        "arn:aws:s3:::jumpstart-cache-prod-us-west-2/*",
        "arn:aws:s3:::jumpstart-cache-prod-us-east-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-us-east-2/*",
        "arn:aws:s3:::jumpstart-cache-prod-eu-west-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-eu-central-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-south-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-northeast-2/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-northeast-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-southeast-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-southeast-2/*"
      ]
    },
    {
      "Sid" : "S3ListOperations",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueOperations",
      "Effect" : "Allow",
      "Action" : "glue:SearchTables",
      "Resource" : [
        "arn:aws:glue:*:*:table/*/*",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:catalog"
      ]
    },
    {
      "Sid" : "SecretsManagerARNBasedOperation",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:CreateSecret",
        "secretsmanager:PutResourcePolicy"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:AmazonSageMaker-*"
```

```
      ]
    },
    {
      "Sid" : "SecretManagerTagBasedOperation",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "RedshiftOperations",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:ExecuteStatement",
        "redshift-data:DescribeStatement",
        "redshift-data:CancelStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables",
        "redshift-data:DescribeTable"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftGetCredentialsOperation",
      "Effect" : "Allow",
      "Action" : [
        "redshift:GetClusterCredentials"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:dbuser:*/sagemaker_access*",
        "arn:aws:redshift:*:*:dbname:*"
      ]
    },
    {
      "Sid" : "ForecastOperations",
      "Effect" : "Allow",
```

```
      "Action" : [
        "forecast:CreateExplainabilityExport",
        "forecast:CreateExplainability",
        "forecast:CreateForecastEndpoint",
        "forecast:CreateAutoPredictor",
        "forecast:CreateDatasetImportJob",
        "forecast:CreateDatasetGroup",
        "forecast:CreateDataset",
        "forecast:CreateForecast",
        "forecast:CreateForecastExportJob",
        "forecast:CreatePredictorBacktestExportJob",
        "forecast:CreatePredictor",
        "forecast:DescribeExplainabilityExport",
        "forecast:DescribeExplainability",
        "forecast:DescribeAutoPredictor",
        "forecast:DescribeForecastEndpoint",
        "forecast:DescribeDatasetImportJob",
        "forecast:DescribeDataset",
        "forecast:DescribeForecast",
        "forecast:DescribeForecastExportJob",
        "forecast:DescribePredictorBacktestExportJob",
        "forecast:GetAccuracyMetrics",
        "forecast:InvokeForecastEndpoint",
        "forecast:GetRecentForecastContext",
        "forecast:DescribePredictor",
        "forecast:TagResource",
        "forecast:DeleteResourceTree"
      ],
      "Resource" : [
        "arn:aws:forecast:*:*:*Canvas*"
      ]
    },
    {
      "Sid" : "RDSOperation",
      "Effect" : "Allow",
      "Action" : "rds:DescribeDBInstances",
      "Resource" : "*"
    },
    {
      "Sid" : "IAMPassOperationForForecast",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
```

```
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "forecast.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AutoscalingOperations",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget"
      ],
      "Resource" : "arn:aws:application-autoscaling:*:*:scalable-target/*",
      "Condition" : {
        "StringEquals" : {
          "application-autoscaling:service-namespace" : "sagemaker",
          "application-autoscaling:scalable-dimension" :
"sagemaker:variant:DesiredInstanceCount"
        }
      }
    },
    {
      "Sid" : "AsyncEndpointOperations",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "sagemaker:DescribeEndpointConfig"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeScalingOperations",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalingActivities"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Sid" : "SageMakerCloudWatchUpdate",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:TargetTracking*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "application-autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AutoscalingSageMakerEndpointOperation",
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "sagemaker.application-autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AthenaOperation",
      "Action" : [
        "athena:ListTableMetadata",
        "athena:ListDataCatalogs",
        "athena:ListDatabases"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
```

```
    {
      "Sid" : "GlueOperation",
      "Action" : [
        "glue:GetDatabases",
        "glue:GetPartitions",
        "glue:GetTables"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "QuicksightOperation",
      "Action" : [
        "quicksight:ListNamespaces"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowUseOfKeyInAccount",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/Source" : "SageMakerCanvas",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "EMRServerlessCreateApplicationOperation",
      "Effect" : "Allow",
      "Action" : "emr-serverless:CreateApplication",
      "Resource" : "arn:aws:emr-serverless:*:*:/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessListApplicationOperation",
      "Effect" : "Allow",
      "Action" : "emr-serverless:ListApplications",
      "Resource" : "arn:aws:emr-serverless:*:*:/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessApplicationOperations",
      "Effect" : "Allow",
      "Action" : [
        "emr-serverless:UpdateApplication",
        "emr-serverless:StopApplication",
        "emr-serverless:GetApplication",
        "emr-serverless:StartApplication"
      ],
      "Resource" : "arn:aws:emr-serverless:*:*:/applications/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessStartJobRunOperation",
```

```
      "Effect" : "Allow",
      "Action" : "emr-serverless:StartJobRun",
      "Resource" : "arn:aws:emr-serverless:*:*:/applications/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessListJobRunOperation",
      "Effect" : "Allow",
      "Action" : "emr-serverless:ListJobRuns",
      "Resource" : "arn:aws:emr-serverless:*:*:/applications/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessJobRunOperations",
      "Effect" : "Allow",
      "Action" : [
        "emr-serverless:GetJobRun",
        "emr-serverless:CancelJobRun"
      ],
      "Resource" : "arn:aws:emr-serverless:*:*:/applications/*/jobruns/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessTagResourceOperation",
      "Effect" : "Allow",
      "Action" : "emr-serverless:TagResource",
      "Resource" : "arn:aws:emr-serverless:*:*:/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:RequestTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "IAMPassOperationForEMRServerless",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSageMakerCanvasEMRSExecutionAccess-*",
        "arn:aws:iam::*:role/AmazonSageMakerCanvasEMRSExecutionAccess-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "emr-serverless.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonSageMakerCanvasSMDataScienceAssistantAccess

説明: Amazon SageMaker Canvas が SageMaker Data Science Assistant サービスを使用するためのアクセス許可を提供します。Data Science Assistant は現在、Amazon SageMaker と Amazon Q Developer の両方を使用してユーザープロンプトを処理しています。

AmazonSageMakerCanvasSMDataScienceAssistantAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに
AmazonSageMakerCanvasSMDataScienceAssistantAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 12 月 4 日 14:06 UTC
- 編集日時: 2025 年 1 月 13 日 22:52 UTC
- ARN: arn:aws:iam::aws:policy/
  AmazonSageMakerCanvasSMDataScienceAssistantAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SageMakerDataScienceAssistantAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker-data-science-assistant:SendConversation"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
```

```
      "Sid" : "AmazonQDeveloperAccess",
      "Effect" : "Allow",
      "Action" : [
        "q:SendMessage",
        "q:StartConversation"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonSageMakerClusterInstanceRolePolicy

説明:このポリシーは、Amazon SageMaker クラスターを使用するために一般的に必要とされるアクセス許可を付与します。

`AmazonSageMakerClusterInstanceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonSageMakerClusterInstanceRolePolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 11 月 29 日 15:11 UTC

- 編集日時: 2023 年 11 月 29 日 15:11 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerClusterInstanceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonSageMakerCoreServiceRolePolicy

説明: Amazon SageMaker Core Services のサービスリンクロールのマネージドポリシー

`AmazonSageMakerCoreServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 12 月 21 日 21:40 UTC
- 編集日時: 2020 年 12 月 21 日 21:40 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSageMakerCoreServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonSageMakerEdgeDeviceFleetPolicy

説明: SageMaker Edge がデフォルトのクラウド接続を使用して顧客のデバイスフリートを作成および管理するために必要なアクセス許可を提供します。

AmazonSageMakerEdgeDeviceFleetPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerEdgeDeviceFleetPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 12 月 8 日 16:17 UTC
- 編集日時: 2020 年 12 月 8 日 16:17 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerEdgeDeviceFleetPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonSageMakerFeatureStoreAccess

説明: Amazon SageMaker FeatureStore 特徴量グループのオフラインストアを有効にするために必要なアクセス許可を提供します。

AmazonSageMakerFeatureStoreAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerFeatureStoreAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 12 月 1 日 16:24 UTC
- 編集日時: 2022 年 12 月 5 日 14:19 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerFeatureStoreAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonSageMakerFullAccess

説明: AWS マネジメントコンソール および SDK 経由で Amazon SageMaker へのフルアクセスを提供します。また、関連サービス (S3、ECR、CloudWatch Logs など) への特定のアクセスも提供します。

`AmazonSageMakerFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 11 月 29 日 13:07 UTC
- 編集日時: 2024 年 12 月 4 日 13:21 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerFullAccess

ポリシーのバージョン

ポリシーのバージョン: v27 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowAllNonAdminSageMakerActions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:*",
        "sagemaker-geospatial:*"
      ],
      "NotResource" : [
        "arn:aws:sagemaker:*:*:domain/*",
        "arn:aws:sagemaker:*:*:user-profile/*",
        "arn:aws:sagemaker:*:*:app/*",
        "arn:aws:sagemaker:*:*:space/*",
        "arn:aws:sagemaker:*:*:partner-app/*",
        "arn:aws:sagemaker:*:*:flow-definition/*",
        "arn:aws:sagemaker:*:*:training-plan/*",
        "arn:aws:sagemaker:*:*:reserved-capacity/*"
```

```
      ]
    },
    {
      "Sid" : "AllowAddTagsForSpace",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:space/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "sagemaker:TaggingAction" : "CreateSpace"
        }
      }
    },
    {
      "Sid" : "AllowAddTagsForApp",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:app/*"
      ]
    },
    {
      "Sid" : "AllowUseOfTrainingPlanResources",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateTrainingJob",
        "sagemaker:CreateCluster",
        "sagemaker:UpdateCluster",
        "sagemaker:DescribeTrainingPlan"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-plan/*",
        "arn:aws:sagemaker:*:*:reserved-capacity/*"
      ]
    },
    {
      "Sid" : "AllowStudioActions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "sagemaker:CreatePresignedDomainUrl",
        "sagemaker:DescribeDomain",
        "sagemaker:ListDomains",
        "sagemaker:DescribeUserProfile",
        "sagemaker:ListUserProfiles",
        "sagemaker:DescribeSpace",
        "sagemaker:ListSpaces",
        "sagemaker:DescribeApp",
        "sagemaker:ListApps"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAppActionsForUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateApp",
        "sagemaker:DeleteApp"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:app/*/*/*/*",
      "Condition" : {
        "Null" : {
          "sagemaker:OwnerUserProfileArn" : "true"
        }
      }
    },
    {
      "Sid" : "AllowAppActionsForSharedSpaces",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateApp",
        "sagemaker:DeleteApp"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:app/${sagemaker:DomainId}/*/*/*",
      "Condition" : {
        "StringEquals" : {
          "sagemaker:SpaceSharingType" : [
            "Shared"
          ]
        }
      }
    },
    {
```

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

```
      "Condition" : {
        "ArnLike" : {
          "sagemaker:OwnerUserProfileArn" : "arn:aws:sagemaker:*:*:user-profile/
${sagemaker:DomainId}/${sagemaker:UserProfileName}"
        },
        "StringEquals" : {
          "sagemaker:SpaceSharingType" : [
            "Private"
          ]
        }
      }
    },
    {
      "Sid" : "AllowFlowDefinitionActions",
      "Effect" : "Allow",
      "Action" : "sagemaker:*",
      "Resource" : [
        "arn:aws:sagemaker:*:*:flow-definition/*"
      ],
      "Condition" : {
        "StringEqualsIfExists" : {
          "sagemaker:WorkteamType" : [
            "private-crowd",
            "vendor-crowd"
          ]
        }
      }
    },
    {
      "Sid" : "AllowAWSServiceActions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeleteScheduledAction",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:PutScheduledAction",
        "application-autoscaling:RegisterScalableTarget",
        "aws-marketplace:ViewSubscriptions",
        "cloudformation:GetTemplateSummary",
```

```
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:PutMetricData",
        "codecommit:BatchGetRepositories",
        "codecommit:CreateRepository",
        "codecommit:GetRepository",
        "codecommit:List*",
        "cognito-idp:AdminAddUserToGroup",
        "cognito-idp:AdminCreateUser",
        "cognito-idp:AdminDeleteUser",
        "cognito-idp:AdminDisableUser",
        "cognito-idp:AdminEnableUser",
        "cognito-idp:AdminRemoveUserFromGroup",
        "cognito-idp:CreateGroup",
        "cognito-idp:CreateUserPool",
        "cognito-idp:CreateUserPoolClient",
        "cognito-idp:CreateUserPoolDomain",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:List*",
        "cognito-idp:UpdateUserPool",
        "cognito-idp:UpdateUserPoolClient",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:CreateVpcEndpoint",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:CreateRepository",
        "ecr:Describe*",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer",
```

```
        "ecr:StartImageScan",
        "elastic-inference:Connect",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets",
        "fsx:DescribeFileSystems",
        "glue:CreateJob",
        "glue:DeleteJob",
        "glue:GetJob*",
        "glue:GetTable*",
        "glue:GetWorkflowRun",
        "glue:ResetJobBookmark",
        "glue:StartJobRun",
        "glue:StartWorkflowRun",
        "glue:UpdateJob",
        "groundtruthlabeling:*",
        "iam:ListRoles",
        "kms:DescribeKey",
        "kms:ListAliases",
        "lambda:ListFunctions",
        "logs:CreateLogDelivery",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DeleteLogDelivery",
        "logs:Describe*",
        "logs:GetLogDelivery",
        "logs:GetLogEvents",
        "logs:ListLogDeliveries",
        "logs:PutLogEvents",
        "logs:PutResourcePolicy",
        "logs:UpdateLogDelivery",
        "robomaker:CreateSimulationApplication",
        "robomaker:DescribeSimulationApplication",
        "robomaker:DeleteSimulationApplication",
        "robomaker:CreateSimulationJob",
        "robomaker:DescribeSimulationJob",
        "robomaker:CancelSimulationJob",
        "secretsmanager:ListSecrets",
        "servicecatalog:Describe*",
        "servicecatalog:List*",
        "servicecatalog:ScanProvisionedProducts",
        "servicecatalog:SearchProducts",
        "servicecatalog:SearchProvisionedProducts",
        "sns:ListTopics",
        "tag:GetResources"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowECRActions",
      "Effect" : "Allow",
      "Action" : [
        "ecr:SetRepositoryPolicy",
        "ecr:CompleteLayerUpload",
        "ecr:BatchDeleteImage",
        "ecr:UploadLayerPart",
        "ecr:DeleteRepositoryPolicy",
        "ecr:InitiateLayerUpload",
        "ecr:DeleteRepository",
        "ecr:PutImage"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/*sagemaker*"
      ]
    },
    {
      "Sid" : "AllowCodeCommitActions",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:GitPull",
        "codecommit:GitPush"
      ],
      "Resource" : [
        "arn:aws:codecommit:*:*:*sagemaker*",
        "arn:aws:codecommit:*:*:*SageMaker*",
        "arn:aws:codecommit:*:*:*Sagemaker*"
      ]
    },
    {
      "Sid" : "AllowCodeBuildActions",
      "Action" : [
        "codebuild:BatchGetBuilds",
        "codebuild:StartBuild"
      ],
      "Resource" : [
        "arn:aws:codebuild:*:*:project/sagemaker*",
        "arn:aws:codebuild:*:*:build/*"
      ],
      "Effect" : "Allow"
```

```
    },
    {
      "Sid" : "AllowStepFunctionsActions",
      "Action" : [
        "states:DescribeExecution",
        "states:GetExecutionHistory",
        "states:StartExecution",
        "states:StopExecution",
        "states:UpdateStateMachine"
      ],
      "Resource" : [
        "arn:aws:states:*:*:statemachine:*sagemaker*",
        "arn:aws:states:*:*:execution:*sagemaker*:*"
      ],
      "Effect" : "Allow"
    },
    {
      "Sid" : "AllowSecretManagerActions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:CreateSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:AmazonSageMaker-*"
      ]
    },
    {
      "Sid" : "AllowReadOnlySecretManagerActions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "AllowServiceCatalogProvisionProduct",
```

```
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:ProvisionProduct"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowServiceCatalogTerminateUpdateProvisionProduct",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:TerminateProvisionedProduct",
        "servicecatalog:UpdateProvisionedProduct"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "servicecatalog:userLevel" : "self"
        }
      }
    },
    {
      "Sid" : "AllowS3ObjectActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:AbortMultipartUpload"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*",
        "arn:aws:s3:::*aws-glue*"
      ]
    },
    {
      "Sid" : "AllowS3GetObjectWithSageMakerExistingObjectTag",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
```

```
      ],
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "AllowS3GetObjectWithServiceCatalogProvisioningExistingObjectTag",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ],
      "Condition" : {
        "StringEquals" : {
          "s3:ExistingObjectTag/servicecatalog:provisioning" : "true"
        }
      }
    },
    {
      "Sid" : "AllowS3BucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketCors",
        "s3:PutBucketCors"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowS3BucketACL",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketAcl",
        "s3:PutObjectAcl"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
```

```
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
      ]
    },
    {
      "Sid" : "AllowLambdaInvokeFunction",
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*SageMaker*",
        "arn:aws:lambda:*:*:function:*sagemaker*",
        "arn:aws:lambda:*:*:function:*Sagemaker*",
        "arn:aws:lambda:*:*:function:*LabelingFunction*"
      ]
    },
    {
      "Sid" : "AllowCreateServiceLinkedRoleForSageMakerApplicationAutoscaling",
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "sagemaker.application-autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowCreateServiceLinkedRoleForRobomaker",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "robomaker.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowSNSActions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "sns:Subscribe",
        "sns:CreateTopic",
        "sns:Publish"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:*SageMaker*",
        "arn:aws:sns:*:*:*Sagemaker*",
        "arn:aws:sns:*:*:*sagemaker*"
      ]
    },
    {
      "Sid" : "AllowPassRoleForSageMakerRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*AmazonSageMaker*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com",
            "robomaker.amazonaws.com",
            "states.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowPassRoleToSageMaker",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "sagemaker.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowAthenaActions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "athena:ListDataCatalogs",
        "athena:ListDatabases",
        "athena:ListTableMetadata",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:StartQueryExecution",
        "athena:StopQueryExecution"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowGlueCreateTable",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateTable"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/*/sagemaker_tmp_*",
        "arn:aws:glue:*:*:table/sagemaker_featurestore/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*"
      ]
    },
    {
      "Sid" : "AllowGlueUpdateTable",
      "Effect" : "Allow",
      "Action" : [
        "glue:UpdateTable"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/sagemaker_featurestore/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/sagemaker_featurestore"
      ]
    },
    {
      "Sid" : "AllowGlueDeleteTable",
      "Effect" : "Allow",
      "Action" : [
        "glue:DeleteTable"
      ],
      "Resource" : [
```

```
        "arn:aws:glue:*:*:table/*/sagemaker_tmp_*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*"
      ]
    },
    {
      "Sid" : "AllowGlueGetTablesAndDatabases",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*"
      ]
    },
    {
      "Sid" : "AllowGlueGetAndCreateDatabase",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:GetDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/sagemaker_featurestore",
        "arn:aws:glue:*:*:database/sagemaker_processing",
        "arn:aws:glue:*:*:database/default",
        "arn:aws:glue:*:*:database/sagemaker_data_wrangler"
      ]
    },
    {
      "Sid" : "AllowRedshiftDataActions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:ExecuteStatement",
        "redshift-data:DescribeStatement",
        "redshift-data:CancelStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables"
```

```
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowRedshiftGetClusterCredentials",
      "Effect" : "Allow",
      "Action" : [
        "redshift:GetClusterCredentials"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:dbuser:*/sagemaker_access*",
        "arn:aws:redshift:*:*:dbname:*"
      ]
    },
    {
      "Sid" : "AllowListTagsForUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:user-profile/*"
      ]
    },
    {
      "Sid" : "AllowCloudformationListStackResources",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStackResources"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/SC-*"
    },
    {
      "Sid" : "AllowS3ExpressObjectActions",
      "Effect" : "Allow",
      "Action" : [
        "s3express:CreateSession"
      ],
      "Resource" : [
        "arn:aws:s3express:*:*:bucket/*SageMaker*",
        "arn:aws:s3express:*:*:bucket/*Sagemaker*",
        "arn:aws:s3express:*:*:bucket/*sagemaker*",
```

```
        "arn:aws:s3express:*:*:bucket/*aws-glue*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowS3ExpressCreateBucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3express:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3express:*:*:bucket/*SageMaker*",
        "arn:aws:s3express:*:*:bucket/*Sagemaker*",
        "arn:aws:s3express:*:*:bucket/*sagemaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowS3ExpressListBucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3express:ListAllMyDirectoryBuckets"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonSageMakerGeospatialExecutionRole

説明: このポリシーは、SageMaker Geospatial を使用するために一般的に必要とされるサービスへのアクセスを提供します。

AmazonSageMakerGeospatialExecutionRole は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerGeospatialExecutionRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 11 月 30 日 10:08 UTC
- 編集日時: 2023 年 5 月 10 日 20:28 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerGeospatialExecutionRole

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonSageMakerGeospatialFullAccess

説明: このポリシーは、 AWS マネジメントコンソール および SDK を介して Amazon SageMaker Geospatial へのフルアクセスを許可するアクセス許可を付与します。

`AmazonSageMakerGeospatialFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonSageMakerGeospatialFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 11 月 30 日 10:06 UTC
- 編集日時: 2022 年 11 月 30 日 10:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerGeospatialFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonSageMakerGroundTruthExecution

説明: SageMaker GroundTruth ラベリングジョブの実行に必要な AWS サービスへのアクセスを提供します

`AmazonSageMakerGroundTruthExecution` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonSageMakerGroundTruthExecution` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 7 月 9 日 19:30 UTC
- 編集日時: 2022 年 4 月 29 日 20:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerGroundTruthExecution`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonSageMakerHyperPodObservabilityAdminAccess

説明: このポリシーは、SageMaker HyperPod オブザーバビリティの設定に必要な管理者特権を提供します。これにより、Amazon Managed Prometheus、Amazon Managed Grafana、および EKS アドオンへのアクセスが可能になります。このポリシーには、アカウント内のすべての Amazon Managed Grafana ワークスペースで ServiceAccountTokens を介した Grafana HTTP API への広範なアクセスも含まれています。

`AmazonSageMakerHyperPodObservabilityAdminAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonSageMakerHyperPodObservabilityAdminAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 7 月 10 日 14:37 UTC
- 編集日時: 2025 年 8 月 21 日 21:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerHyperPodObservabilityAdminAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PrometheusCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "aps:CreateWorkspace"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "PrometheusTagsAccess",
      "Effect" : "Allow",
      "Action" : "aps:TagResource",
      "Resource" : [
        "arn:aws:aps:*:*:/workspaces",
```

```
        "arn:aws:aps:*:*:rulegroupsnamespace/*/HyperPodObservabilityNamespace"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SageMaker"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/SageMaker" : "true",
          "aws:ResourceTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "PrometheusDescribeAccess",
      "Effect" : "Allow",
      "Action" : [
        "aps:DescribeWorkspace"
      ],
      "Resource" : "arn:aws:aps:*:*:workspace/*"
    },
    {
      "Sid" : "PrometheusListAccess",
      "Effect" : "Allow",
      "Action" : [
        "aps:ListWorkspaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PrometheusAlertsRuleGroupAccess",
      "Effect" : "Allow",
      "Action" : [
        "aps:CreateAlertManagerDefinition",
        "aps:DescribeAlertManagerDefinition",
        "aps:DescribeRuleGroupsNamespace",
        "aps:ListRuleGroupsNamespaces"
      ],
      "Resource" : [
        "arn:aws:aps:*:*:workspace/*",
        "arn:aws:aps:*:*:rulegroupsnamespace/*/HyperPodObservabilityNamespace"
      ]
    },
```

```
    {
      "Sid" : "PrometheusCreateRuleGroupAccess",
      "Effect" : "Allow",
      "Action" : "aps:CreateRuleGroupsNamespace",
      "Resource" : "arn:aws:aps:*:*:rulegroupsnamespace/*/
HyperPodObservabilityNamespace",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SageMaker" : "true",
          "aws:ResourceTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "GrafanaCreateWorkspaceAccess",
      "Effect" : "Allow",
      "Action" : [
        "grafana:CreateWorkspace"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "GrafanaTagsAccess",
      "Effect" : "Allow",
      "Action" : "grafana:TagResource",
      "Resource" : "arn:aws:grafana:*:*:/workspaces",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SageMaker"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/SageMaker" : "true",
          "aws:ResourceTag/SageMaker" : "true"
        }
      }
    },
    {
```

```
      "Sid" : "GrafanaListAccess",
      "Effect" : "Allow",
      "Action" : [
        "grafana:ListWorkspaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GrafanaServiceAccountAccess",
      "Effect" : "Allow",
      "Action" : [
        "grafana:DescribeWorkspace",
        "grafana:CreateWorkspaceApiKey",
        "grafana:CreateWorkspaceServiceAccount",
        "grafana:CreateWorkspaceServiceAccountToken",
        "grafana:ListWorkspaceServiceAccounts",
        "grafana:ListWorkspaceServiceAccountTokens",
        "grafana:DeleteWorkspaceServiceAccountToken"
      ],
      "Resource" : "arn:aws:grafana:*:*:/workspaces/*"
    },
    {
      "Sid" : "IAMGrafanaPassRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSageMakerHyperPodObservabilityGrafanaAccess-*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "grafana.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "IAMEKSPassRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
```

```
      "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSageMakerHyperPodObservabilityAddonAccess-*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "pods.eks.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "IAMGetRoleAccess",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerHyperPodObservabilityAddonAccess-*"
      ]
    },
    {
      "Sid" : "HyperPodClusterAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListClusters",
        "sagemaker:DescribeCluster"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EKSAddonAccess",
      "Effect" : "Allow",
      "Action" : [
        "eks:DeleteAddon",
        "eks:UpdateAddon",
        "eks:DescribeAddon"
      ],
      "Resource" : "arn:aws:eks:*:*:addon/*/amazon-sagemaker-hyperpod-observability/*"
    },
    {
      "Sid" : "EKSAddonDescribeAccess",
      "Effect" : "Allow",
      "Action" : [
        "eks:DescribeAddonConfiguration",
        "eks:DescribeAddonVersions"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EKSAddonPodIdentityAccess",
      "Effect" : "Allow",
      "Action" : [
        "eks:DescribePodIdentityAssociation",
        "eks:DeletePodIdentityAssociation",
        "eks:UpdatePodIdentityAssociation"
      ],
      "Resource" : "arn:aws:eks:*:*:podidentityassociation/*/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "EKSListDescribeAccess",
      "Effect" : "Allow",
      "Action" : [
        "eks:ListAddons",
        "eks:DescribeCluster"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/*"
    },
    {
      "Sid" : "EKSCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "eks:CreateAddon",
        "eks:CreatePodIdentityAssociation"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "EKSTagsAccess",
      "Effect" : "Allow",
```

```
      "Action" : "eks:TagResource",
      "Resource" : [
        "arn:aws:eks:*:*:cluster/*",
        "arn:aws:eks:*:*:addon/*/*/*",
        "arn:aws:eks:*:*:podidentityassociation/*/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SageMaker"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/SageMaker" : "true",
          "aws:ResourceTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "SSOAccess",
      "Effect" : "Allow",
      "Action" : [
        "sso:DescribeRegisteredRegions",
        "sso:CreateManagedApplicationInstance"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonSageMakerHyperPodServiceRolePolicy

説明: このポリシーは、Amazon EKS、Amazon CloudWatch などの関連サービスに対するアクセス許可を Amazon SageMaker HyperPod に付与します。 AWS Amazon CloudWatch

AmazonSageMakerHyperPodServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2024 年 9 月 6 日 17:04 UTC
- 編集日時: 2024 年 9 月 6 日 17:04 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonSageMakerHyperPodServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
      "Action" : "eks:DescribeCluster",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogGroupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/sagemaker/Clusters/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogStreamPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/sagemaker/Clusters/*:log-stream:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonSageMakerHyperPodTrainingOperatorAccess

説明: このポリシーは、SageMaker HyperPod トレーニングオペレーターをセットアップするために必要な管理アクセス許可を提供します。Amazon SageMaker HyperPod および EKS アドオンへのアクセスを有効にします。このポリシーには、アカウントの SageMaker HyperPod リソースを記述するアクセス許可が含まれています。

AmazonSageMakerHyperPodTrainingOperatorAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerHyperPodTrainingOperatorAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 8 月 19 日 17:04 UTC
- 編集日時: 2025 年 8 月 19 日 17:04 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerHyperPodTrainingOperatorAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
      "Effect" : "Allow",
      "Action" : "sagemaker:DescribeClusterNode",
      "Resource" : "arn:aws:sagemaker:*:*:cluster/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SageMaker" : "true"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonSageMakerMechanicalTurkAccess

説明: 任意のワークチームに対して Amazon Augmented AI FlowDefinition リソースを作成するためのアクセスを提供します。

`AmazonSageMakerMechanicalTurkAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonSageMakerMechanicalTurkAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 12 月 3 日 16:19 UTC
- 編集日時: 2019 年 12 月 3 日 16:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerMechanicalTurkAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonSageMakerModelGovernanceUseAccess

説明: この AWS 管理ポリシーは、すべての Amazon SageMaker ガバナンス機能を使用するために必要なアクセス許可を付与します。このポリシーは、関連サービス (S3、KMS など) への限定アクセスも提供します。

AmazonSageMakerModelGovernanceUseAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerModelGovernanceUseAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 11 月 30 日 08:58 UTC
- 編集日時: 2024 年 6 月 4 日 21:48 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerModelGovernanceUseAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonSageMakerModelRegistryFullAccess

説明: これは、Sagemaker の Model Registry 向けの新しいマネージドポリシーです。このポリシーは、ユーザーロールにアタッチして Sagemaker のモデルレジストリ関連の機能にアクセスできるスタンドアロンポリシーです。

`AmazonSageMakerModelRegistryFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonSageMakerModelRegistryFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 4 月 13 日 05:20 UTC

- 編集日時: 2024 年 6 月 6 日 18:48 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerModelRegistryFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonSageMakerNotebooksServiceRolePolicy

説明: Amazon SageMaker Notebooks のサービスリンクロール向けマネージドポリシー

AmazonSageMakerNotebooksServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 10 月 18 日 20:27 UTC
- 編集日時: 2025 年 12 月 10 日 18:34 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonSageMakerNotebooksServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v11 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
        "fsx:DescribeFileSystems"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowSageMakerDeleteApp",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DeleteApp"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:app/*"
    },
    {
      "Sid" : "AllowEFSAccessPointCreation",
      "Effect" : "Allow",
      "Action" : "elasticfilesystem:CreateAccessPoint",
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/ManagedByAmazonSageMakerResource" : "*",
          "aws:RequestTag/ManagedByAmazonSageMakerResource" : "*"
        }
      }
    },
    {
      "Sid" : "AllowEFSAccessPointDeletion",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DeleteAccessPoint"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:access-point/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/ManagedByAmazonSageMakerResource" : "*"
        }
      }
    },
    {
      "Sid" : "AllowEFSCreation",
```

```
      "Effect" : "Allow",
      "Action" : "elasticfilesystem:CreateFileSystem",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/ManagedByAmazonSageMakerResource" : "*"
        }
      }
    },
    {
      "Sid" : "AllowEFSMountWithDeletion",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:CreateMountTarget",
        "elasticfilesystem:DeleteFileSystem",
        "elasticfilesystem:DeleteMountTarget"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/ManagedByAmazonSageMakerResource" : "*"
        }
      }
    },
    {
      "Sid" : "AllowEFSDescribe",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowEFSTagging",
      "Effect" : "Allow",
      "Action" : "elasticfilesystem:TagResource",
      "Resource" : [
        "arn:aws:elasticfilesystem:*:*:access-point/*",
        "arn:aws:elasticfilesystem:*:*:file-system/*"
      ],
      "Condition" : {
        "StringLike" : {
```

```
          "aws:ResourceTag/ManagedByAmazonSageMakerResource" : "*"
        }
      }
    },
    {
      "Sid" : "AllowEC2Tagging",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "AllowEC2Operations",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowEC2AuthZ",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
```

```
          "ec2:ResourceTag/ManagedByAmazonSageMakerResource" : "*"
        }
      }
    },
    {
      "Sid" : "AllowIdcOperations",
      "Effect" : "Allow",
      "Action" : [
        "sso:CreateManagedApplicationInstance",
        "sso:DeleteManagedApplicationInstance",
        "sso:GetManagedApplicationInstance"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:*:sso:::instance/*"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityStore",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
"arn:*:identitystore::*:identitystore/*"
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
```

```
        }
      }
    },
    {
      "Sid" : "AllowSagemakerProfileCreation",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateUserProfile",
        "sagemaker:DescribeUserProfile"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSagemakerSpaceOperationsForCanvasManagedSpaces",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateSpace",
        "sagemaker:DescribeSpace",
        "sagemaker:DeleteSpace",
        "sagemaker:ListTags"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:space/*/CanvasManagedSpace-*"
    },
    {
      "Sid" : "AllowSagemakerAddTagsForAppManagedSpaces",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:space/*/CanvasManagedSpace-*",
      "Condition" : {
        "StringEquals" : {
          "sagemaker:TaggingAction" : "CreateSpace"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonSageMakerPartnerAppsFullAccess

説明: Amazon SageMaker パートナーアプリケーションユーザーがアプリケーションにアクセスし、利用可能なアプリケーションを一覧表示し、アプリケーションウェブ UI を起動し、アプリケーション SDK 経由で接続できるようにします。

`AmazonSageMakerPartnerAppsFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonSageMakerPartnerAppsFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 1 月 17 日 18:37 UTC
- 編集日時: 2025 年 1 月 17 日 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerPartnerAppsFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonSageMakerPartnerListAppsPermission",
      "Effect" : "Allow",
      "Action" : "sagemaker:ListPartnerApps",
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "AmazonSageMakerPartnerAppsPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreatePartnerAppPresignedUrl",
        "sagemaker:DescribePartnerApp",
        "sagemaker:CallPartnerAppApi"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : "arn:aws:sagemaker:*:*:partner-app/*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceR

説明: Amazon SageMaker 製品ポートフォリオの AWS ServiceCatalog プロビジョニング製品内の AWS APIGateway で使用されるサービスロールポリシー。 Amazon SageMaker Lambda などを含む一連の関連サービスにアクセス許可を付与します。

AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 8 月 1 日 15:06 UTC
- 編集日時: 2023 年 8 月 1 日 15:06 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServi

説明: Amazon SageMaker 製品ポートフォリオの AWS ServiceCatalog プロビジョニング製品内で AWS CloudFormation が使用するサービスロールポリシー。Lambda、APIGateway などの関連サービスのサブセットにアクセス許可を付与します。

`AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 8 月 1 日 15:06 UTC

- 編集日時: 2023 年 8 月 1 日 15:06 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRoleP

説明: Amazon SageMaker 製品ポートフォリオの AWS ServiceCatalog プロビジョニング製品内で AWS Lambda が使用するサービスロールポリシー。Secrets Manager などを含む一連の関連サービスにアクセス許可を付与します。

AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 8 月 1 日 15:05 UTC
- 編集日時: 2023 年 8 月 1 日 15:05 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonSageMakerPipelinesIntegrations

説明: この Amazon マネージドポリシーは、SageMaker モデル構築パイプラインのコールバックステップと Lambda ステップでの使用に一般的に必要とされるアクセス許可を付与します。SageMaker Studio のセットアップ時に作成できる AmazonSageMaker-ExecutionRole に追加されます。パイプラインの作成または実行に使用される他のロールにアタッチすることもできます。

`AmazonSageMakerPipelinesIntegrations` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonSageMakerPipelinesIntegrations` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 7 月 30 日 16:35 UTC
- 編集日時: 2023 年 2 月 17 日 21:28 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonSageMakerQuickSightVPCPolicy

説明: このポリシーは、SageMaker Unified Studio が QuickSight の VPC 関連リソースを作成するために使用します。

`AmazonSageMakerQuickSightVPCPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonSageMakerQuickSightVPCPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2025 年 6 月 3 日 17:37 UTC
- 編集日時: 2025 年 6 月 3 日 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerQuickSightVPCPolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ManageQuickSightVPCConnection",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:CreateVPCConnection",
        "quicksight:DescribeVPCConnection",
        "quicksight:DeleteVPCConnection",
        "quicksight:ListVPCConnections",
        "quicksight:UpdateVPCConnection"
      ],
      "Resource" : "arn:aws:quicksight:*:*:vpcconnection/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "DescribeQuickSightVPCConnectionEC2Resources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
```

```
      "Sid" : "ManageQuickSightEC2NetworkInterface",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonSageMakerReadOnly

説明: AWS マネジメントコンソール および SDK 経由で Amazon SageMaker への読み取り専用アクセスを提供します。

`AmazonSageMakerReadOnly` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonSageMakerReadOnly` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 11 月 29 日 13:07 UTC
- 編集日時: 2021 年 12 月 1 日 16:29 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerReadOnly`

ポリシーのバージョン

ポリシーのバージョン: v11 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePoli

説明: Amazon SageMaker 製品ポートフォリオの AWS ServiceCatalog プロビジョニング製品内の AWS APIGateway で使用されるサービスロールポリシー。 Amazon SageMaker CloudWatch Logs やその他の関連サービスのセットにアクセス許可を付与します。

`AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 3 月 25 日 04:25 UTC
- 編集日時: 2022 年 3 月 25 日 04:25 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonSageMakerServiceCatalogProductsCloudformationServiceRoleP

説明: Amazon SageMaker 製品ポートフォリオの AWS ServiceCatalog プロビジョニング製品内で AWS CloudFormation が使用するサービスロールポリシー。SageMaker やその他の関連サービスの一部にアクセス許可を付与します。

AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー

- 作成日時: 2022 年 3 月 25 日 04:26 UTC
- 編集日時: 2022 年 3 月 25 日 04:26 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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"
      ]
    }
```

```
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy

説明: Amazon SageMaker 製品ポートフォリオの AWS ServiceCatalog プロビジョニング製品内で AWS CodeBuild が使用するサービスロールポリシー。CodePipeline、CodeBuild などを含む関連サービスのサブセットにアクセス許可を付与します。

`AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 3 月 25 日 04:27 UTC
- 編集日時: 2025 年 9 月 27 日 04:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonSageMakerCodeBuildCodeCommitPermission",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:CancelUploadArchive",
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetUploadArchiveStatus",
        "codecommit:UploadArchive"
      ],
      "Resource" : "arn:aws:codecommit:*:*:sagemaker-*"
    },
    {
      "Sid" : "AmazonSageMakerCodeBuildECRReadPermission",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:DescribeImageScanFindings",
        "ecr:DescribeRegistry",
        "ecr:DescribeImageReplicationStatus",
        "ecr:DescribeRepositories",
        "ecr:DescribeImageReplicationStatus",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerCodeBuildECRWritePermission",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ecr:CompleteLayerUpload",
        "ecr:CreateRepository",
        "ecr:InitiateLayerUpload",
        "ecr:PutImage",
        "ecr:UploadLayerPart"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerCodeBuildPassRoletPermission",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsEventsRole",
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsCodePipelineRole",
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsCloudformationRole",
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsCodeBuildRole",
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsExecutionRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "events.amazonaws.com",
            "codepipeline.amazonaws.com",
            "cloudformation.amazonaws.com",
            "codebuild.amazonaws.com",
            "sagemaker.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerCodeBuildLogPermission",
      "Effect" : "Allow",
      "Action" : [
```

```
        "logs:CreateLogDelivery",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DeleteLogDelivery",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:DescribeResourcePolicies",
        "logs:DescribeDestinations",
        "logs:DescribeExportTasks",
        "logs:DescribeMetricFilters",
        "logs:DescribeQueries",
        "logs:DescribeQueryDefinitions",
        "logs:DescribeSubscriptionFilters",
        "logs:GetLogDelivery",
        "logs:GetLogEvents",
        "logs:ListLogDeliveries",
        "logs:PutLogEvents",
        "logs:PutResourcePolicy",
        "logs:UpdateLogDelivery"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/codebuild/*"
    },
    {
      "Sid" : "AmazonSageMakerCodeBuildS3Permission",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:GetBucketAcl",
        "s3:GetBucketCors",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:PutBucketCors",
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*",
        "arn:aws:s3:::sagemaker-*"
```

```
      ]
    },
    {
      "Sid" : "AmazonSageMakerCodeBuildSageMakerPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddAssociation",
        "sagemaker:AddTags",
        "sagemaker:AssociateTrialComponent",
        "sagemaker:BatchDescribeModelPackage",
        "sagemaker:BatchGetMetrics",
        "sagemaker:BatchGetRecord",
        "sagemaker:BatchPutMetrics",
        "sagemaker:CreateAction",
        "sagemaker:CreateAlgorithm",
        "sagemaker:CreateApp",
        "sagemaker:CreateAppImageConfig",
        "sagemaker:CreateArtifact",
        "sagemaker:CreateAutoMLJob",
        "sagemaker:CreateCodeRepository",
        "sagemaker:CreateCompilationJob",
        "sagemaker:CreateContext",
        "sagemaker:CreateDataQualityJobDefinition",
        "sagemaker:CreateDeviceFleet",
        "sagemaker:CreateDomain",
        "sagemaker:CreateEdgePackagingJob",
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateExperiment",
        "sagemaker:CreateFeatureGroup",
        "sagemaker:CreateFlowDefinition",
        "sagemaker:CreateHumanTaskUi",
        "sagemaker:CreateHyperParameterTuningJob",
        "sagemaker:CreateImage",
        "sagemaker:CreateImageVersion",
        "sagemaker:CreateInferenceRecommendationsJob",
        "sagemaker:CreateLabelingJob",
        "sagemaker:CreateLineageGroupPolicy",
        "sagemaker:CreateModel",
        "sagemaker:CreateModelBiasJobDefinition",
        "sagemaker:CreateModelExplainabilityJobDefinition",
        "sagemaker:CreateModelPackage",
        "sagemaker:CreateModelPackageGroup",
        "sagemaker:CreateModelQualityJobDefinition",
```

```
        "sagemaker:CreateMonitoringSchedule",
        "sagemaker:CreateNotebookInstance",
        "sagemaker:CreateNotebookInstanceLifecycleConfig",
        "sagemaker:CreatePipeline",
        "sagemaker:CreatePresignedDomainUrl",
        "sagemaker:CreatePresignedNotebookInstanceUrl",
        "sagemaker:CreateProcessingJob",
        "sagemaker:CreateProject",
        "sagemaker:CreateTrainingJob",
        "sagemaker:CreateTransformJob",
        "sagemaker:CreateTrial",
        "sagemaker:CreateTrialComponent",
        "sagemaker:CreateUserProfile",
        "sagemaker:CreateWorkforce",
        "sagemaker:CreateWorkteam",
        "sagemaker:DeleteAction",
        "sagemaker:DeleteAlgorithm",
        "sagemaker:DeleteApp",
        "sagemaker:DeleteAppImageConfig",
        "sagemaker:DeleteArtifact",
        "sagemaker:DeleteAssociation",
        "sagemaker:DeleteCodeRepository",
        "sagemaker:DeleteContext",
        "sagemaker:DeleteDataQualityJobDefinition",
        "sagemaker:DeleteDeviceFleet",
        "sagemaker:DeleteDomain",
        "sagemaker:DeleteEndpoint",
        "sagemaker:DeleteEndpointConfig",
        "sagemaker:DeleteExperiment",
        "sagemaker:DeleteFeatureGroup",
        "sagemaker:DeleteFlowDefinition",
        "sagemaker:DeleteHumanLoop",
        "sagemaker:DeleteHumanTaskUi",
        "sagemaker:DeleteImage",
        "sagemaker:DeleteImageVersion",
        "sagemaker:DeleteLineageGroupPolicy",
        "sagemaker:DeleteModel",
        "sagemaker:DeleteModelBiasJobDefinition",
        "sagemaker:DeleteModelExplainabilityJobDefinition",
        "sagemaker:DeleteModelPackage",
        "sagemaker:DeleteModelPackageGroup",
        "sagemaker:DeleteModelPackageGroupPolicy",
        "sagemaker:DeleteModelQualityJobDefinition",
        "sagemaker:DeleteMonitoringSchedule",
```

```
        "sagemaker:DeleteNotebookInstance",
        "sagemaker:DeleteNotebookInstanceLifecycleConfig",
        "sagemaker:DeletePipeline",
        "sagemaker:DeleteProject",
        "sagemaker:DeleteRecord",
        "sagemaker:DeleteTags",
        "sagemaker:DeleteTrial",
        "sagemaker:DeleteTrialComponent",
        "sagemaker:DeleteUserProfile",
        "sagemaker:DeleteWorkforce",
        "sagemaker:DeleteWorkteam",
        "sagemaker:DeregisterDevices",
        "sagemaker:DescribeAction",
        "sagemaker:DescribeAlgorithm",
        "sagemaker:DescribeApp",
        "sagemaker:DescribeAppImageConfig",
        "sagemaker:DescribeArtifact",
        "sagemaker:DescribeAutoMLJob",
        "sagemaker:DescribeCodeRepository",
        "sagemaker:DescribeCompilationJob",
        "sagemaker:DescribeContext",
        "sagemaker:DescribeDataQualityJobDefinition",
        "sagemaker:DescribeDevice",
        "sagemaker:DescribeDeviceFleet",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeEdgePackagingJob",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeExperiment",
        "sagemaker:DescribeFeatureGroup",
        "sagemaker:DescribeFlowDefinition",
        "sagemaker:DescribeHumanLoop",
        "sagemaker:DescribeHumanTaskUi",
        "sagemaker:DescribeHyperParameterTuningJob",
        "sagemaker:DescribeImage",
        "sagemaker:DescribeImageVersion",
        "sagemaker:DescribeInferenceRecommendationsJob",
        "sagemaker:DescribeLabelingJob",
        "sagemaker:DescribeLineageGroup",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeModelBiasJobDefinition",
        "sagemaker:DescribeModelExplainabilityJobDefinition",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
```

```
        "sagemaker:DescribeModelQualityJobDefinition",
        "sagemaker:DescribeMonitoringSchedule",
        "sagemaker:DescribeNotebookInstance",
        "sagemaker:DescribeNotebookInstanceLifecycleConfig",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribePipelineDefinitionForExecution",
        "sagemaker:DescribePipelineExecution",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeProject",
        "sagemaker:DescribeSubscribedWorkteam",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:DescribeTransformJob",
        "sagemaker:DescribeTrial",
        "sagemaker:DescribeTrialComponent",
        "sagemaker:DescribeUserProfile",
        "sagemaker:DescribeWorkforce",
        "sagemaker:DescribeWorkteam",
        "sagemaker:DisableSagemakerServicecatalogPortfolio",
        "sagemaker:DisassociateTrialComponent",
        "sagemaker:EnableSagemakerServicecatalogPortfolio",
        "sagemaker:GetDeviceFleetReport",
        "sagemaker:GetDeviceRegistration",
        "sagemaker:GetLineageGroupPolicy",
        "sagemaker:GetModelPackageGroupPolicy",
        "sagemaker:GetRecord",
        "sagemaker:GetSagemakerServicecatalogPortfolioStatus",
        "sagemaker:GetSearchSuggestions",
        "sagemaker:InvokeEndpoint",
        "sagemaker:InvokeEndpointAsync",
        "sagemaker:ListActions",
        "sagemaker:ListAlgorithms",
        "sagemaker:ListAppImageConfigs",
        "sagemaker:ListApps",
        "sagemaker:ListArtifacts",
        "sagemaker:ListAssociations",
        "sagemaker:ListAutoMLJobs",
        "sagemaker:ListCandidatesForAutoMLJob",
        "sagemaker:ListCodeRepositories",
        "sagemaker:ListCompilationJobs",
        "sagemaker:ListContexts",
        "sagemaker:ListDataQualityJobDefinitions",
        "sagemaker:ListDeviceFleets",
        "sagemaker:ListDevices",
        "sagemaker:ListDomains",
```

```
        "sagemaker:ListEdgePackagingJobs",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListEndpoints",
        "sagemaker:ListExperiments",
        "sagemaker:ListFeatureGroups",
        "sagemaker:ListFlowDefinitions",
        "sagemaker:ListHumanLoops",
        "sagemaker:ListHumanTaskUis",
        "sagemaker:ListHyperParameterTuningJobs",
        "sagemaker:ListImageVersions",
        "sagemaker:ListImages",
        "sagemaker:ListInferenceRecommendationsJobs",
        "sagemaker:ListLabelingJobs",
        "sagemaker:ListLabelingJobsForWorkteam",
        "sagemaker:ListLineageGroups",
        "sagemaker:ListModelBiasJobDefinitions",
        "sagemaker:ListModelExplainabilityJobDefinitions",
        "sagemaker:ListModelMetadata",
        "sagemaker:ListModelPackageGroups",
        "sagemaker:ListModelPackages",
        "sagemaker:ListModelQualityJobDefinitions",
        "sagemaker:ListModels",
        "sagemaker:ListMonitoringExecutions",
        "sagemaker:ListMonitoringSchedules",
        "sagemaker:ListNotebookInstanceLifecycleConfigs",
        "sagemaker:ListNotebookInstances",
        "sagemaker:ListPipelineExecutionSteps",
        "sagemaker:ListPipelineExecutions",
        "sagemaker:ListPipelineParametersForExecution",
        "sagemaker:ListPipelines",
        "sagemaker:ListProcessingJobs",
        "sagemaker:ListProjects",
        "sagemaker:ListSubscribedWorkteams",
        "sagemaker:ListTags",
        "sagemaker:ListTrainingJobs",
        "sagemaker:ListTrainingJobsForHyperParameterTuningJob",
        "sagemaker:ListTransformJobs",
        "sagemaker:ListTrialComponents",
        "sagemaker:ListTrials",
        "sagemaker:ListUserProfiles",
        "sagemaker:ListWorkforces",
        "sagemaker:ListWorkteams",
        "sagemaker:PutLineageGroupPolicy",
        "sagemaker:PutModelPackageGroupPolicy",
```

```
        "sagemaker:PutRecord",
        "sagemaker:QueryLineage",
        "sagemaker:RegisterDevices",
        "sagemaker:RenderUiTemplate",
        "sagemaker:Search",
        "sagemaker:SendHeartbeat",
        "sagemaker:SendPipelineExecutionStepFailure",
        "sagemaker:SendPipelineExecutionStepSuccess",
        "sagemaker:StartHumanLoop",
        "sagemaker:StartMonitoringSchedule",
        "sagemaker:StartNotebookInstance",
        "sagemaker:StartPipelineExecution",
        "sagemaker:StopAutoMLJob",
        "sagemaker:StopCompilationJob",
        "sagemaker:StopEdgePackagingJob",
        "sagemaker:StopHumanLoop",
        "sagemaker:StopHyperParameterTuningJob",
        "sagemaker:StopInferenceRecommendationsJob",
        "sagemaker:StopLabelingJob",
        "sagemaker:StopMonitoringSchedule",
        "sagemaker:StopNotebookInstance",
        "sagemaker:StopPipelineExecution",
        "sagemaker:StopProcessingJob",
        "sagemaker:StopTrainingJob",
        "sagemaker:StopTransformJob",
        "sagemaker:UpdateAction",
        "sagemaker:UpdateAppImageConfig",
        "sagemaker:UpdateArtifact",
        "sagemaker:UpdateCodeRepository",
        "sagemaker:UpdateContext",
        "sagemaker:UpdateDeviceFleet",
        "sagemaker:UpdateDevices",
        "sagemaker:UpdateDomain",
        "sagemaker:UpdateEndpoint",
        "sagemaker:UpdateEndpointWeightsAndCapacities",
        "sagemaker:UpdateExperiment",
        "sagemaker:UpdateImage",
        "sagemaker:UpdateModelPackage",
        "sagemaker:UpdateMonitoringSchedule",
        "sagemaker:UpdateNotebookInstance",
        "sagemaker:UpdateNotebookInstanceLifecycleConfig",
        "sagemaker:UpdatePipeline",
        "sagemaker:UpdatePipelineExecution",
        "sagemaker:UpdateProject",
```

```
        "sagemaker:UpdateTrainingJob",
        "sagemaker:UpdateTrial",
        "sagemaker:UpdateTrialComponent",
        "sagemaker:UpdateUserProfile",
        "sagemaker:UpdateWorkforce",
        "sagemaker:UpdateWorkteam"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:model/*",
        "arn:aws:sagemaker:*:*:pipeline/*",
        "arn:aws:sagemaker:*:*:project/*",
        "arn:aws:sagemaker:*:*:model-package/*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerCodeBuildCodeStarConnectionPermission",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection"
      ],
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ],
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "aws:ResourceTag/sagemaker" : "true"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerCodeBuildCodeConnectionPermission",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:UseConnection"
      ],
      "Resource" : [
        "arn:aws:codeconnections:*:*:connection/*",
        "arn:aws:codestar-connections:*:*:connection/*"
      ],
      "Condition" : {
        "StringEqualsIgnoreCase" : {
```

```
          "aws:ResourceTag/sagemaker" : "true"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePo

説明: Amazon SageMaker 製品ポートフォリオの AWS ServiceCatalog プロビジョニング製品内で AWS CodePipeline が使用するサービスロールポリシー。CodePipeline、CodeBuild などを含む関連サービスのサブセットにアクセス許可を付与します。

AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 2 月 22 日 09:53 UTC
- 編集日時: 2025 年 9 月 27 日 04:34 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonSageMakerCodePipelineCFnPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:CreateStack",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:SetStackPolicy",
        "cloudformation:UpdateStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/sagemaker-*"
    },
    {
      "Sid" : "AmazonSageMakerCodePipelineCFnTagPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/sagemaker-*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "sagemaker:project-name"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "AmazonSageMakerCodePipelineS3Permission",
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerCodePipelinePassRolePermission",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsCloudformationRole"
      ]
    },
    {
      "Sid" : "AmazonSageMakerCodePipelineCodeBuildPermission",
      "Effect" : "Allow",
      "Action" : [
        "codebuild:BatchGetBuilds",
        "codebuild:StartBuild"
      ],
      "Resource" : [
        "arn:aws:codebuild:*:*:project/sagemaker-*",
        "arn:aws:codebuild:*:*:build/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerCodePipelineCodeCommitPermission",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:CancelUploadArchive",
```

```
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetUploadArchiveStatus",
        "codecommit:UploadArchive"
      ],
      "Resource" : "arn:aws:codecommit:*:*:sagemaker-*"
    },
    {
      "Sid" : "AmazonSageMakerCodePipelineCodeStarConnectionPermission",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection"
      ],
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ],
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "aws:ResourceTag/sagemaker" : "true"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerCodePipelineCodeConnectionPermission",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:UseConnection"
      ],
      "Resource" : [
        "arn:aws:codeconnections:*:*:connection/*",
        "arn:aws:codestar-connections:*:*:connection/*"
      ],
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "aws:ResourceTag/sagemaker" : "true"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy

説明: Amazon SageMaker 製品ポートフォリオの AWS ServiceCatalog プロビジョニング製品内の AWS CloudWatch Events によって使用されるサービスロールポリシー。CodePipeline やその他を含む関連サービスのサブセットにアクセス許可を付与します。

AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 2 月 22 日 09:53 UTC
- 編集日時: 2022 年 2 月 22 日 09:53 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy

説明: Amazon SageMaker 製品ポートフォリオの AWS ServiceCatalog プロビジョニング製品内で AWS Firehose が使用するサービスロールポリシー。Firehose などを含む一連の関連サービスにアクセス許可を付与します。

AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー

- 作成日時: 2022 年 2 月 22 日 09:54 UTC
- 編集日時: 2022 年 2 月 22 日 09:54 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : "arn:aws:firehose:*:*:deliverystream/sagemaker-*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy

説明: Amazon AWS SageMaker 製品ポートフォリオの AWS ServiceCatalog プロビジョニング製品内で Glue が使用するサービスロールポリシー。 Amazon SageMaker このポリシーは、Glue やその他を含めた一連の関連サービスにアクセス許可を付与します。

AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 2 月 22 日 09:51 UTC
- 編集日時: 2022 年 8 月 26 日 19:13 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する

- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy

説明: Amazon SageMaker 製品ポートフォリオの AWS ServiceCatalog プロビジョニング製品内で AWS Lambda が使用するサービスロールポリシー。ECR、S3、その他を含む一連の関連サービスにアクセス許可を付与します。

AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 4 月 4 日 16:34 UTC
- 編集日時: 2024 年 6 月 11 日 18:57 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonSageMakerSpacesControllerPolicy

説明: EKS SageMaker Spaces への安全なリモートアクセスを可能にするために SageMaker Spaces アドオンに必要な Systems Manager のアクティベーション、セッション管理SageMaker キーオペレーションのアクセス許可を付与します。

`AmazonSageMakerSpacesControllerPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonSageMakerSpacesControllerPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 11 月 19 日 04:34 UTC
- 編集日時: 2025 年 11 月 19 日 04:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerSpacesControllerPolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowOperatorToSSMCreateActivationForSpaces",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateActivation"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker.amazonaws.com/managed-by" : "amazon-sagemaker-
spaces",
          "aws:RequestTag/sagemaker.amazonaws.com/eks-cluster-arn" :
 "${aws:PrincipalTag/eks-cluster-arn}"
        }
      }
    },
    {
      "Sid" : "AllowOperatorToSSMDescribeActivations",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeActivations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowOperatorToSSMDescribeSessions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeSessions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowOperatorToSSMDeleteActivation",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteActivation"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "AllowOperatorToAddTagsToActivation",
      "Effect" : "Allow",
      "Action" : "ssm:AddTagsToResource",
      "Resource" : [
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:iam::*:role/sagemaker-space-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker.amazonaws.com/managed-by" : "amazon-sagemaker-
spaces",
          "aws:RequestTag/sagemaker.amazonaws.com/eks-cluster-arn" :
 "${aws:PrincipalTag/eks-cluster-arn}"
        }
      }
    },
    {
      "Sid" : "AllowOperatorToSSMDescribeManagedNodes",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowOperatorToSSMDeregisterWorkspaceInstances",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeregisterManagedInstance"
      ],
      "Resource" : "arn:aws:ssm:*:*:managed-instance/*",
      "Condition" : {
        "StringEquals" : {
          "ssm:resourceTag/sagemaker.amazonaws.com/managed-by" : "amazon-sagemaker-
spaces",
          "ssm:resourceTag/sagemaker.amazonaws.com/eks-cluster-arn" :
 "${aws:PrincipalTag/eks-cluster-arn}"
        }
      }
    },
    {
```

```
      "Sid" : "AllowOperatorToPassSsmManagedNodeRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/sagemaker-space-*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowOperatorToSSMStartSession",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : "arn:aws:ssm:*:*:managed-instance/*",
      "Condition" : {
        "StringEquals" : {
          "ssm:resourceTag/sagemaker.amazonaws.com/managed-by" : "amazon-sagemaker-
spaces",
          "ssm:resourceTag/sagemaker.amazonaws.com/eks-cluster-arn" :
 "${aws:PrincipalTag/eks-cluster-arn}"
        }
      }
    },
    {
      "Sid" : "AllowStartSessionDocuments",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
        "arn:aws:ssm:*::document/AWS-StartSSHSession",
        "arn:aws:ssm:*:*:document/SageMaker-Space*"
      ]
    },
    {
      "Sid" : "KMSDescribeKey",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*"
```

```
    },
    {
      "Sid" : "KMSKeyOperations",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "kms:EncryptionContext:sagemaker:component" : "amazon-sagemaker-spaces",
          "kms:EncryptionContext:sagemaker:eks-cluster-arn" : "${aws:PrincipalTag/eks-
cluster-arn}"
        }
      }
    },
    {
      "Sid" : "AllowOperatorToSSMDescribeDocument",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/SageMaker-Space*"
      ]
    },
    {
      "Sid" : "AllowOperatorToSSMCreateDocument",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateDocument"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/SageMaker-Space*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker.amazonaws.com/managed-by" : "amazon-sagemaker-
spaces",
          "aws:RequestTag/sagemaker.amazonaws.com/eks-cluster-arn" :
 "${aws:PrincipalTag/eks-cluster-arn}"
        }
      }
    },
    {
```

```
      "Sid" : "AllowOperatorToEnableAdvancedTierForManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting",
        "ssm:ResetServiceSetting"
      ],
      "Resource" : "arn:aws:ssm:*:*:servicesetting/ssm/managed-instance/activation-
tier"
    },
    {
      "Sid" : "AllowOperatorToAddTagsToSSMDocument",
      "Effect" : "Allow",
      "Action" : "ssm:AddTagsToResource",
      "Resource" : "arn:aws:ssm:*:*:document/SageMaker-Space*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker.amazonaws.com/managed-by" : "amazon-sagemaker-
spaces"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonSageMakerSpacesRouterPolicy

説明: EKS SageMaker Spaces への安全なリモートアクセスを可能にするために SageMaker Spaces ルーターに必要な Systems KMS キーオペレーションのアクセス許可を付与します。

AmazonSageMakerSpacesRouterPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerSpacesRouterPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 11 月 19 日 04:34 UTC
- 編集日時: 2025 年 11 月 19 日 04:34 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerSpacesRouterPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "KMSDescribeKey",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
      "Sid" : "KMSKeyOperations",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
```

```
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "kms:EncryptionContext:sagemaker:component" : "amazon-sagemaker-spaces",
          "kms:EncryptionContext:sagemaker:eks-cluster-arn" : "${aws:PrincipalTag/eks-
cluster-arn}"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonSageMakerTrainingPlanCreateAccess

説明: この Amazon マネージドポリシーは、SageMaker トレーニングプランを作成および管理するために必要なアクセス許可を提供します。これにより、ユーザーはトレーニングプランとリザーブドキャパシティを作成し、既存のトレーニングプランを記述し、検索および一覧表示オペレーションを実行できます。

AmazonSageMakerTrainingPlanCreateAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerTrainingPlanCreateAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 12 月 4 日 13:21 UTC

- 編集日時: 2025 年 8 月 8 日 21:19 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerTrainingPlanCreateAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateTrainingPlanPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateTrainingPlan",
        "sagemaker:CreateReservedCapacity",
        "sagemaker:DescribeReservedCapacity"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-plan/*",
        "arn:aws:sagemaker:*:*:reserved-capacity/*"
      ]
    },
    {
      "Sid" : "AddTagsToTrainingPlanPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-plan/*",
        "arn:aws:sagemaker:*:*:reserved-capacity/*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "sagemaker:TaggingAction" : [
            "CreateTrainingPlan",
            "CreateReservedCapacity"
          ]
        }
      }
    },
    {
      "Sid" : "DescribeTrainingPlanPermissions",
      "Effect" : "Allow",
      "Action" : "sagemaker:DescribeTrainingPlan",
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-plan/*"
      ]
    },
    {
      "Sid" : "NonResourceLevelTrainingPlanPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:SearchTrainingPlanOfferings",
        "sagemaker:ListTrainingPlans"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListUltraServersByReservedCapacityPermissions",
      "Effect" : "Allow",
      "Action" : "sagemaker:ListUltraServersByReservedCapacity",
      "Resource" : [
        "arn:aws:sagemaker:*:*:reserved-capacity/*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonSecurityLakeAdministrator

説明: Amazon Security Lake と、Security Lake の管理に必要な関連サービスへのフルアクセスを提供します。

AmazonSecurityLakeAdministrator は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSecurityLakeAdministrator をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 5 月 30 日 22:04 UTC
- 編集日時: 2024 年 2 月 23 日 16:01 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSecurityLakeAdministrator

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonSecurityLakeMetastoreManager

説明: Cloudwatch、S3、Glue、SQS へのアクセスを許可する Amazon SecurityLake メタストアマネージャー Lambda のポリシー。

AmazonSecurityLakeMetastoreManager は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSecurityLakeMetastoreManager をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2024 年 1 月 23 日 15:26 UTC
- 編集日時: 2024 年 4 月 01 日 20:04 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSecurityLakeMetastoreManager

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonSecurityLakePermissionsBoundary

説明: Amazon Security Lake は、サードパーティのカスタムソースがデータレイクにデータを書き込むことができるよう、またサードパーティのサブスクライバーがデータレイクのデータを消費することができるように IAM ロールを作成しますが、これらのロールを作成する際にこのポリシーを使用してアクセス許可の範囲を定義します。

`AmazonSecurityLakePermissionsBoundary` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonSecurityLakePermissionsBoundary` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 11 月 29 日 14:11 UTC
- 編集日時: 2024 年 5 月 14 日 20:39 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSecurityLakePermissionsBoundary`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonSESFullAccess

説明: 経由で Amazon SES へのフルアクセスを提供します AWS マネジメントコンソール。

`AmazonSESFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonSESFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2015 年 2 月 6 日 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSESFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonSESReadOnlyAccess

説明: 経由で Amazon SES への読み取り専用アクセスを提供します AWS マネジメントコンソール。

`AmazonSESReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonSESReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2024 年 5 月 14 日 12:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSESReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonSESServiceRolePolicy

説明: SES がお客様の SES リソースに代わって Amazon CloudWatch の基本的なモニタリングメトリクスを公開できるようにします

AmazonSESServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2024 年 5 月 21 日 16:02 UTC
- 編集日時: 2024 年 5 月 21 日 16:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSESServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
```

```
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonSNSFullAccess

説明: 経由で Amazon SNS へのフルアクセスを提供します AWS マネジメントコンソール。

AmazonSNSFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSNSFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2024 年 9 月 24 日 22:32 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSNSFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SNSFullAccess",
      "Effect" : "Allow",
      "Action" : "sns:*",
      "Resource" : "*"
    },
    {
      "Sid" : "SMSAccessViaSNS",
      "Effect" : "Allow",
      "Action" : [
        "sms-voice:DescribeVerifiedDestinationNumbers",
        "sms-voice:CreateVerifiedDestinationNumber",
        "sms-voice:SendDestinationNumberVerificationCode",
        "sms-voice:SendTextMessage",
        "sms-voice:DeleteVerifiedDestinationNumber",
        "sms-voice:VerifyDestinationNumber",
        "sms-voice:DescribeAccountAttributes",
        "sms-voice:DescribeSpendLimits",
        "sms-voice:DescribePhoneNumbers",
        "sms-voice:SetTextMessageSpendLimitOverride",
        "sms-voice:DescribeOptedOutNumbers",
        "sms-voice:DeleteOptedOutNumber"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "sns.amazonaws.com"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonSNSReadOnlyAccess

説明: 経由で Amazon SNS への読み取り専用アクセスを提供します AWS マネジメントコンソール。

AmazonSNSReadOnlyAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSNSReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2024 年 9 月 24 日 22:13 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSNSReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SNSReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:GetTopicAttributes",
        "sns:List*",
        "sns:CheckIfPhoneNumberIsOptedOut",
        "sns:GetEndpointAttributes",
```

```
        "sns:GetDataProtectionPolicy",
        "sns:GetPlatformApplicationAttributes",
        "sns:GetSMSAttributes",
        "sns:GetSMSSandboxAccountStatus",
        "sns:GetSubscriptionAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SMSAccessViaSNS",
      "Effect" : "Allow",
      "Action" : [
        "sms-voice:DescribeVerifiedDestinationNumbers",
        "sms-voice:DescribeAccountAttributes",
        "sms-voice:DescribeSpendLimits",
        "sms-voice:DescribePhoneNumbers",
        "sms-voice:DescribeOptedOutNumbers"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "sns.amazonaws.com"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonSNSRole

説明: Amazon SNS サービスロールのデフォルトポリシー。

AmazonSNSRole は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSNSRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2015 年 2 月 6 日 18:41 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSNSRole

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:PutMetricFilter",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonSQSFullAccess

説明: 経由で Amazon SQS へのフルアクセスを提供します AWS マネジメントコンソール。

AmazonSQSFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSQSFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2015 年 2 月 6 日 18:41 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSQSFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
    {
      "Action" : [
        "sqs:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonSQSReadOnlyAccess

説明: 経由で Amazon SQS への読み取り専用アクセスを提供します AWS マネジメントコンソール。

`AmazonSQSReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonSQSReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2024 年 5 月 24 日 18:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSQSReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonSQSReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ListDeadLetterSourceQueues",
        "sqs:ListQueues",
        "sqs:ListMessageMoveTasks",
        "sqs:ListQueueTags"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonSSMAutomationApproverAccess

説明: 自動化実行を表示し、承認待ちの承認決定を自動化に送信するためのアクセスを提供します

AmazonSSMAutomationApproverAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSSMAutomationApproverAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 8 月 7 日 23:07 UTC
- 編集日時: 2017 年 8 月 7 日 23:07 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSSMAutomationApproverAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonSSMAutomationRole

説明: EC2 Automation Service に、自動化ドキュメント内で定義されたアクティビティを実行する権限を付与します

AmazonSSMAutomationRole は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSSMAutomationRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2016 年 12 月 5 日 22:09 UTC
- 編集日時: 2025 年 9 月 11 日 17:34 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSSMAutomationRole

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : [
        "arn:*:ssm:*:*:session/*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonSSMDirectoryServiceAccess

説明: このポリシーにより、SSM エージェントは顧客に代わって Directory Service にアクセスし、マネージドインスタンスをドメインに参加させることができるようになります。

AmazonSSMDirectoryServiceAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSSMDirectoryServiceAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 3 月 15 日 17:44 UTC
- 編集日時: 2019 年 3 月 15 日 17:44 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMDirectoryServiceAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonSSMFullAccess

説明: Amazon SSM へのフルアクセスを提供します。

AmazonSSMFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSSMFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 5 月 29 日 17:39 UTC
- 編集日時: 2019 年 11 月 20 日 20:08 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSSMFullAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonSSMMaintenanceWindowRole

説明: EC2 メンテナンスウィンドウに使用されるサービスロール

AmazonSSMMaintenanceWindowRole は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSSMMaintenanceWindowRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2016 年 12 月 1 日 15:57 UTC
- 編集日時: 2019 年 7 月 27 日 00:16 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSSMMaintenanceWindowRole

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonSSMManagedEC2InstanceDefaultPolicy

説明: このポリシーは、EC2 インスタンスで AWS Systems Manager 機能を有効にします。

`AmazonSSMManagedEC2InstanceDefaultPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonSSMManagedEC2InstanceDefaultPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 8 月 30 日 20:54 UTC
- 編集日時: 2024 年 7 月 16 日 18:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMManagedEC2InstanceDefaultPolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSSMAgentPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAssociation",
        "ssm:GetDeployablePatchSnapshotForInstance",
        "ssm:GetDocument",
        "ssm:DescribeDocument",
        "ssm:GetManifest",
        "ssm:ListAssociations",
        "ssm:ListInstanceAssociations",
        "ssm:PutInventory",
        "ssm:PutComplianceItems",
        "ssm:PutConfigurePackageResult",
        "ssm:UpdateAssociationStatus",
        "ssm:UpdateInstanceAssociationStatus",
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSSMChannelMessaging",
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSSMLegacyMessaging",
      "Effect" : "Allow",
      "Action" : [
        "ec2messages:AcknowledgeMessage",
        "ec2messages:DeleteMessage",
        "ec2messages:FailMessage",
```

```
        "ec2messages:GetEndpoint",
        "ec2messages:GetMessages",
        "ec2messages:SendReply"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonSSMManagedInstanceCore

説明: AWS Systems Manager サービスコア機能を有効にする Amazon EC2 ロールのポリシー。

`AmazonSSMManagedInstanceCore` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonSSMManagedInstanceCore` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 3 月 15 日 17:22 UTC
- 編集日時: 2019 年 5 月 23 日 16:54 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonSSMPatchAssociation

説明: パッチ関連付け操作用の子インスタンスへのアクセス権を提供します。

AmazonSSMPatchAssociation は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSSMPatchAssociation をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 5 月 13 日 16:00 UTC
- 編集日時: 2020 年 5 月 13 日 16:00 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSSMPatchAssociation

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonSSMReadOnlyAccess

説明: Amazon SSM への読み取り専用アクセスを提供します。

AmazonSSMReadOnlyAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSSMReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 5 月 29 日 17:44 UTC
- 編集日時: 2015 年 5 月 29 日 17:44 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSSMReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
        "ssm:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonSSMServiceRolePolicy

説明: Amazon SSM が管理または使用する AWS リソースへのアクセスを提供します

`AmazonSSMServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 11 月 13 日 19:20 UTC
- 編集日時: 2025 年 7 月 15 日 17:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSSMServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v16 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CancelCommand",
        "ssm:GetCommandInvocation",
        "ssm:ListCommandInvocations",
        "ssm:ListCommands",
        "ssm:SendCommand",
        "ssm:GetAutomationExecution",
        "ssm:GetParameters",
        "ssm:StartAutomationExecution",
        "ssm:StopAutomationExecution",
        "ssm:ListTagsForResource",
        "ssm:GetCalendarState"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutInventory"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "ssm:InventoryTypeName" : [
            "AWS:ComplianceItem",
            "AWS:PatchSummary"
          ]
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/*",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:SSM*",
        "arn:aws:lambda:*:*:function:*:SSM*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "states:DescribeExecution",
        "states:StartExecution"
      ],
      "Resource" : [
        "arn:aws:states:*:*:stateMachine:SSM*",
        "arn:aws:states:*:*:execution:SSM*"
      ]
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:ListGroups",
        "resource-groups:ListGroupResources",
        "resource-groups:GetGroupQuery"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:SelectResourceConfig"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "compute-optimizer:GetEC2InstanceRecommendations",
```

```
        "compute-optimizer:GetEnrollmentStatus"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "support:DescribeTrustedAdvisorChecks",
        "support:DescribeTrustedAdvisorCheckSummaries",
        "support:DescribeTrustedAdvisorCheckResult",
        "support:DescribeCases"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeComplianceByConfigRule",
        "config:DescribeComplianceByResource",
        "config:DescribeRemediationConfigurations",
        "config:DescribeConfigurationRecorders"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:DescribeAlarms",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "organizations:DescribeOrganization",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudformation:ListStackSets",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStackInstances",
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:DeleteStackSet"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stackset/AWS-QuickSetup-SSM*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudformation:DeleteStackInstances",
      "Resource" : [
        "arn:aws:cloudformation:*:*:stackset/AWS-QuickSetup-SSM*:*",
        "arn:aws:cloudformation:*:*:stackset-target/AWS-QuickSetup-SSM*:*",
        "arn:aws:cloudformation:*:*:type/resource/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "ssm.amazonaws.com"
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "events:RemoveTargets",
        "events:DeleteRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/SSMExplorerManagedRule"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "events:DescribeRule",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "securityhub:DescribeHub",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "resource-explorer-2:CreateManagedView",
      "Resource" : "arn:aws:resource-explorer-2:*:*:managed-view/AWSManagedViewForSSM*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonSumerianFullAccess

説明: Amazon Sumerian へのフルアクセスを提供します。

`AmazonSumerianFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSumerianFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 4 月 24 日 20:14 UTC
- 編集日時: 2018 年 4 月 24 日 20:14 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSumerianFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonTextractFullAccess

説明: すべての Amazon Textract API へのアクセス

AmazonTextractFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonTextractFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 11 月 28 日 19:07 UTC
- 編集日時: 2018 年 11 月 28 日 19:07 UTC
- ARN: arn:aws:iam::aws:policy/AmazonTextractFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonTextractServiceRole

説明: Textract がユーザーに代わって AWS サービスを呼び出すことを許可します。

AmazonTextractServiceRole は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonTextractServiceRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2018 年 11 月 28 日 19:12 UTC
- 編集日時: 2018 年 11 月 28 日 19:12 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonTextractServiceRole

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonTimestreamConsoleFullAccess

説明: AWS マネジメントコンソールを使用して Amazon Timestream を管理するためのフルアクセスを提供します。このポリシーでは、特定の KMS オペレーションや、保存したクエリを管理する操作に対するアクセス許可も付与されることに注意してください。カスタマー管理型 CMK を使用している場合は、必要な追加のアクセス許可についてドキュメントを参照してください。

`AmazonTimestreamConsoleFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonTimestreamConsoleFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2020 年 9 月 30 日 21:47 UTC
- 編集日時: 2025 年 10 月 16 日 14:34 UTC
- ARN: arn:aws:iam::aws:policy/AmazonTimestreamConsoleFullAccess

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "timestream:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListKeys",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : [
        "arn:aws:kms:*:*:key/*"
      ],
```

```
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:timestream:database-name"
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        },
        "StringLike" : {
          "kms:ViaService" : "timestream.*.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dbqms:CreateFavoriteQuery",
        "dbqms:DescribeFavoriteQueries",
        "dbqms:UpdateFavoriteQuery",
        "dbqms:DeleteFavoriteQueries",
        "dbqms:GetQueryString",
        "dbqms:CreateQueryHistory",
        "dbqms:DescribeQueryHistory",
        "dbqms:UpdateQueryHistory",
        "dbqms:DeleteQueryHistory"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics",
        "iam:ListRoles"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "pricing:GetProducts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSMarketplaceViewSubscriptions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ViewSubscriptions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AWSMarketplaceAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:SearchAgreements",
        "aws-marketplace:AcceptAgreementRequest",
        "aws-marketplace:CreateAgreementRequest",
        "aws-marketplace:ListEntitlementDetails",
        "aws-marketplace:DescribeAgreement",
        "aws-marketplace:Subscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws-marketplace:ProductId" : [
            "prod-xcc5llpq4vlbc",
            "prod-5jijo74ujy36m",
            "prod-rjppt7huo35fm"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonTimestreamFullAccess

説明: Amazon Timestream へのフルアクセスを提供します。このポリシーでは、特定の KMS オペレーションへのアクセス許可も付与されることに注意してください。カスタマー管理型 CMK を使用している場合は、必要な追加のアクセス許可についてドキュメントを参照してください。

`AmazonTimestreamFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonTimestreamFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 9 月 30 日 21:47 UTC
- 編集日時: 2021 年 11 月 26 日 23:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
```

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonTimestreamInfluxDBFullAccess

説明: Amazon Timestream InfluxDB インスタンスを作成、更新、削除、一覧表示し、パラメータグループを作成、一覧表示するための完全な管理者アクセスを提供します。追加で必要となるアクセス許可についてはドキュメントを参照してください。

`AmazonTimestreamInfluxDBFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonTimestreamInfluxDBFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 3 月 14 日 22:53 UTC
- 編集日時: 2025 年 12 月 16 日 20:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamInfluxDBFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TimestreamInfluxDBStatement",
      "Effect" : "Allow",
      "Action" : [
        "timestream-influxdb:CreateDbParameterGroup",
        "timestream-influxdb:GetDbParameterGroup",
        "timestream-influxdb:ListDbParameterGroups",
        "timestream-influxdb:CreateDbInstance",
        "timestream-influxdb:DeleteDbInstance",
        "timestream-influxdb:GetDbInstance",
        "timestream-influxdb:ListDbInstances",
        "timestream-influxdb:TagResource",
        "timestream-influxdb:UntagResource",
        "timestream-influxdb:ListTagsForResource",
        "timestream-influxdb:UpdateDbInstance",
        "timestream-influxdb:CreateDbCluster",
        "timestream-influxdb:GetDbCluster",
        "timestream-influxdb:UpdateDbCluster",
        "timestream-influxdb:DeleteDbCluster",
        "timestream-influxdb:ListDbClusters",
        "timestream-influxdb:ListDbInstancesForCluster",
        "timestream-influxdb:RebootDbInstance",
        "timestream-influxdb:RebootDbCluster"
      ],
      "Resource" : "arn:aws:timestream-influxdb:*:*:*"
    },
    {
      "Sid" : "ServiceLinkedRoleStatement",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/timestream-
influxdb.amazonaws.com/AWSServiceRoleForTimestreamInfluxDB",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "timestream-influxdb.amazonaws.com"
        }
      }
    },
```

```
    {
      "Sid" : "NetworkValidationStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateEniInSubnetStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BucketValidationStatement",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ]
    },
    {
      "Sid" : "MPViewAccessStatement",
      "Effect" : "Allow",
      "Action" : [
```

```
        "aws-marketplace:ViewSubscriptions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MPSubscriptionAccessStatement",
      "Effect" : "Allow",
      "Action" : "aws-marketplace:Subscribe",
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws-marketplace:ProductId" : [
            "prod-xcc5llpq4vlbc",
            "prod-rjppt7huo35fm"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonTimestreamInfluxDBFullAccessWithoutMarketplaceAccess

説明: マーケットプレイスオペレーションを除く Amazon Timestream InfluxDB インスタンスとパラメータグループを管理するための管理アクセスを提供します。

`AmazonTimestreamInfluxDBFullAccessWithoutMarketplaceAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonTimestreamInfluxDBFullAccessWithoutMarketplaceAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 4 月 17 日 17:52 UTC
- 編集日時: 2025 年 12 月 16 日 20:34 UTC
- ARN: arn:aws:iam::aws:policy/AmazonTimestreamInfluxDBFullAccessWithoutMarketplaceAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TimestreamInfluxDBStatement",
      "Effect" : "Allow",
      "Action" : [
        "timestream-influxdb:CreateDbParameterGroup",
        "timestream-influxdb:GetDbParameterGroup",
        "timestream-influxdb:ListDbParameterGroups",
        "timestream-influxdb:CreateDbInstance",
        "timestream-influxdb:DeleteDbInstance",
        "timestream-influxdb:GetDbInstance",
        "timestream-influxdb:ListDbInstances",
        "timestream-influxdb:TagResource",
        "timestream-influxdb:UntagResource",
```

```
        "timestream-influxdb:ListTagsForResource",
        "timestream-influxdb:UpdateDbInstance",
        "timestream-influxdb:CreateDbCluster",
        "timestream-influxdb:GetDbCluster",
        "timestream-influxdb:UpdateDbCluster",
        "timestream-influxdb:DeleteDbCluster",
        "timestream-influxdb:ListDbClusters",
        "timestream-influxdb:ListDbInstancesForCluster",
        "timestream-influxdb:RebootDbInstance",
        "timestream-influxdb:RebootDbCluster"
      ],
      "Resource" : [
        "arn:aws:timestream-influxdb:*:*:*"
      ]
    },
    {
      "Sid" : "ServiceLinkedRoleStatement",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/timestream-
influxdb.amazonaws.com/AWSServiceRoleForTimestreamInfluxDB",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "timestream-influxdb.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "NetworkValidationStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CreateEniInSubnetStatement",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BucketValidationStatement",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonTimestreamInfluxDBServiceRolePolicy

説明: Amazon Timestream InfluxDB インスタンスを作成、更新、削除、一覧表示し、パラメータグループを作成、一覧表示するための完全な管理者アクセスを提供します。追加で必要となるアクセス許可についてはドキュメントを参照してください。

AmazonTimestreamInfluxDBServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2024 年 3 月 14 日 18:53 UTC
- 編集日時: 2024 年 3 月 14 日 18:53 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonTimestreamInfluxDBServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonTimestreamReadOnlyAccess

説明: Amazon Timestream への読み取り専用アクセスを提供します。ポリシーには、実行中のクエリをキャンセルするアクセス許可も付与されます。カスタマー管理型 CMK を使用している場合は、必要な追加のアクセス許可についてドキュメントを参照してください。

`AmazonTimestreamReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonTimestreamReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 9 月 30 日 21:47 UTC
- 編集日時: 2024 年 6 月 5 日 19:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonTranscribeFullAccess

説明: Amazon Transcribe オペレーションへのフルアクセスを提供します

AmazonTranscribeFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonTranscribeFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 4 月 4 日 16:06 UTC
- 編集日時: 2018 年 4 月 4 日 16:06 UTC
- ARN: arn:aws:iam::aws:policy/AmazonTranscribeFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "transcribe:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*transcribe*"
```

```
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonTranscribeReadOnlyAccess

説明: Amazon Transcribe の読み取り専用オペレーションへのアクセスを提供します

`AmazonTranscribeReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonTranscribeReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 4 月 4 日 16:05 UTC
- 編集日時: 2018 年 4 月 4 日 16:05 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTranscribeReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonVerifiedPermissionsFullAccess

説明: Verified Permissions へのフルアクセスを提供します

`AmazonVerifiedPermissionsFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonVerifiedPermissionsFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 10 月 11 日 18:19 UTC

- 編集日時: 2024 年 10 月 11 日 18:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVerifiedPermissionsFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AccountLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "verifiedpermissions:CreatePolicyStore",
        "verifiedpermissions:ListPolicyStores"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PolicyStoreLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "verifiedpermissions:*"
      ],
      "Resource" : [
        "arn:aws:verifiedpermissions::*:policy-store/*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する

- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonVerifiedPermissionsReadOnlyAccess

説明: Verified Permissions サービスへの読み取り専用アクセスを提供します。

AmazonVerifiedPermissionsReadOnlyAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonVerifiedPermissionsReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 10 月 11 日 18:25 UTC
- 編集日時: 2024 年 10 月 11 日 18:25 UTC
- ARN: arn:aws:iam::aws:policy/AmazonVerifiedPermissionsReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
      "Action" : [
        "verifiedpermissions:ListPolicyStores"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PolicyStoreLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "verifiedpermissions:GetIdentitySource",
        "verifiedpermissions:GetPolicy",
        "verifiedpermissions:GetPolicyStore",
        "verifiedpermissions:GetPolicyTemplate",
        "verifiedpermissions:GetSchema",
        "verifiedpermissions:IsAuthorized",
        "verifiedpermissions:IsAuthorizedWithToken",
        "verifiedpermissions:ListIdentitySources",
        "verifiedpermissions:ListPolicies",
        "verifiedpermissions:ListPolicyTemplates"
      ],
      "Resource" : [
        "arn:aws:verifiedpermissions::*:policy-store/*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonVPCCrossAccountNetworkInterfaceOperations

説明: ネットワークインターフェイスを作成し、クロスアカウントリソースにアタッチするためのアクセス許可を付与

AmazonVPCCrossAccountNetworkInterfaceOperations は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonVPCCrossAccountNetworkInterfaceOperations をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 7 月 18 日 20:47 UTC
- 編集日時: 2023 年 9 月 25 日 15:12 UTC
- ARN: arn:aws:iam::aws:policy/AmazonVPCCrossAccountNetworkInterfaceOperations

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonVPCFullAccess

説明: 経由で Amazon VPC へのフルアクセスを提供します AWS マネジメントコンソール。

`AmazonVPCFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonVPCFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2024 年 12 月 9 日 17:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v11 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
      "Sid" : "AmazonVPCFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AcceptVpcPeeringConnection",
        "ec2:AcceptVpcEndpointConnections",
        "ec2:AllocateAddress",
        "ec2:AssignIpv6Addresses",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssociateAddress",
        "ec2:AssociateDhcpOptions",
        "ec2:AssociateRouteTable",
        "ec2:AssociateSecurityGroupVpc",
        "ec2:AssociateSubnetCidrBlock",
        "ec2:AssociateVpcCidrBlock",
        "ec2:AttachClassicLinkVpc",
        "ec2:AttachInternetGateway",
        "ec2:AttachNetworkInterface",
        "ec2:AttachVpnGateway",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateCarrierGateway",
        "ec2:CreateCustomerGateway",
        "ec2:CreateDefaultSubnet",
        "ec2:CreateDefaultVpc",
        "ec2:CreateDhcpOptions",
        "ec2:CreateEgressOnlyInternetGateway",
        "ec2:CreateFlowLogs",
        "ec2:CreateInternetGateway",
        "ec2:CreateLocalGatewayRouteTableVpcAssociation",
        "ec2:CreateNatGateway",
        "ec2:CreateNetworkAcl",
        "ec2:CreateNetworkAclEntry",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateTags",
        "ec2:CreateVpc",
        "ec2:CreateVpcEndpoint",
        "ec2:CreateVpcEndpointConnectionNotification",
        "ec2:CreateVpcEndpointServiceConfiguration",
        "ec2:CreateVpcPeeringConnection",
```

```
        "ec2:CreateVpnConnection",
        "ec2:CreateVpnConnectionRoute",
        "ec2:CreateVpnGateway",
        "ec2:DeleteCarrierGateway",
        "ec2:DeleteCustomerGateway",
        "ec2:DeleteDhcpOptions",
        "ec2:DeleteEgressOnlyInternetGateway",
        "ec2:DeleteFlowLogs",
        "ec2:DeleteInternetGateway",
        "ec2:DeleteLocalGatewayRouteTableVpcAssociation",
        "ec2:DeleteNatGateway",
        "ec2:DeleteNetworkAcl",
        "ec2:DeleteNetworkAclEntry",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteSubnet",
        "ec2:DeleteTags",
        "ec2:DeleteVpc",
        "ec2:DeleteVpcEndpoints",
        "ec2:DeleteVpcEndpointConnectionNotifications",
        "ec2:DeleteVpcEndpointServiceConfigurations",
        "ec2:DeleteVpcPeeringConnection",
        "ec2:DeleteVpnConnection",
        "ec2:DeleteVpnConnectionRoute",
        "ec2:DeleteVpnGateway",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCarrierGateways",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeIpv6Pools",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeMovingAddresses",
```

```
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupReferences",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSecurityGroupVpcAssociations",
        "ec2:DescribeStaleSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeVpcClassicLinkDnsSupport",
        "ec2:DescribeVpcEndpointConnectionNotifications",
        "ec2:DescribeVpcEndpointConnections",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpointServicePermissions",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:DetachClassicLinkVpc",
        "ec2:DetachInternetGateway",
        "ec2:DetachNetworkInterface",
        "ec2:DetachVpnGateway",
        "ec2:DisableVgwRoutePropagation",
        "ec2:DisableVpcClassicLink",
        "ec2:DisableVpcClassicLinkDnsSupport",
        "ec2:DisassociateAddress",
        "ec2:DisassociateRouteTable",
        "ec2:DisassociateSecurityGroupVpc",
        "ec2:DisassociateSubnetCidrBlock",
        "ec2:DisassociateVpcCidrBlock",
        "ec2:EnableVgwRoutePropagation",
        "ec2:EnableVpcClassicLink",
        "ec2:EnableVpcClassicLinkDnsSupport",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:ModifyNetworkInterfaceAttribute",
```

```
        "ec2:ModifySecurityGroupRules",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:ModifyVpcEndpoint",
        "ec2:ModifyVpcEndpointConnectionNotification",
        "ec2:ModifyVpcEndpointServiceConfiguration",
        "ec2:ModifyVpcEndpointServicePermissions",
        "ec2:ModifyVpcPeeringConnectionOptions",
        "ec2:ModifyVpcTenancy",
        "ec2:MoveAddressToVpc",
        "ec2:RejectVpcEndpointConnections",
        "ec2:RejectVpcPeeringConnection",
        "ec2:ReleaseAddress",
        "ec2:ReplaceNetworkAclAssociation",
        "ec2:ReplaceNetworkAclEntry",
        "ec2:ReplaceRoute",
        "ec2:ReplaceRouteTableAssociation",
        "ec2:ResetNetworkInterfaceAttribute",
        "ec2:RestoreAddressToClassic",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:UnassignIpv6Addresses",
        "ec2:UnassignPrivateIpAddresses",
        "ec2:UpdateSecurityGroupRuleDescriptionsEgress",
        "ec2:UpdateSecurityGroupRuleDescriptionsIngress"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonVPCNetworkAccessAnalyzerFullAccessPolicy

説明: AWS リソースを記述し、Network Access Analyzer を実行し、Network Insights アクセススコープと Network Insights アクセススコープ分析でタグを作成または削除するためのアクセス許可を提供します。

AmazonVPCNetworkAccessAnalyzerFullAccessPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonVPCNetworkAccessAnalyzerFullAccessPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 6 月 15 日 22:56 UTC
- 編集日時: 2024 年 5 月 15 日 21:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonVPCNetworkAccessAnalyzerFullAccessPolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonVPCReachabilityAnalyzerFullAccessPolicy

説明: AWS リソースを記述し、Reachability Analyzer を実行し、Network Insights パスと Network Insights Analysis でタグを作成または削除するためのアクセス許可を提供します。

`AmazonVPCReachabilityAnalyzerFullAccessPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonVPCReachabilityAnalyzerFullAccessPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 6 月 14 日 20:12 UTC
- 編集日時: 2024 年 5 月 15 日 20:47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCReachabilityAnalyzerFullAccessPolicy`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonVPCReachabilityAnalyzerPathComponentReadPolicy

説明: このポリシーは、IAMRoleForReachabilityAnalyzerCrossAccountResourceAccess というロールにアタッチされています。管理アカウントが Reachability Analyzer に対して信頼できるアクセスを有効にすると、このロールは組織のメンバーアカウントに展開されます。Reachability Analyzer コンソールを使用して組織全体のリソースを表示するためのアクセス許可を付与します。

`AmazonVPCReachabilityAnalyzerPathComponentReadPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonVPCReachabilityAnalyzerPathComponentReadPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 5 月 1 日 20:38 UTC
- 編集日時: 2023 年 5 月 1 日 20:38 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCReachabilityAnalyzerPathComponentReadPolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonVPCReadOnlyAccess

説明: 経由で Amazon VPC への読み取り専用アクセスを提供します AWS マネジメントコンソール。

`AmazonVPCReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonVPCReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC

- 編集日時: 2024 年 12 月 9 日 15:06 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v10 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonVPCReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeCarrierGateways",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeMovingAddresses",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupReferences",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
```

```
        "ec2:DescribeSecurityGroupVpcAssociations",
        "ec2:DescribeStaleSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeVpcClassicLinkDnsSupport",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointConnectionNotifications",
        "ec2:DescribeVpcEndpointConnections",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpointServicePermissions",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetSecurityGroupsForVpc"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonWorkDocsFullAccess

説明: 経由で Amazon WorkDocs へのフルアクセスを提供します AWS マネジメントコンソール

`AmazonWorkDocsFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonWorkDocsFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 4 月 16 日 23:05 UTC
- 編集日時: 2020 年 4 月 16 日 23:05 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkDocsFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "workdocs:*",
        "ds:DescribeDirectories",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonWorkDocsReadOnlyAccess

説明: 経由で Amazon WorkDocs への読み取り専用アクセスを提供します AWS マネジメントコンソール

AmazonWorkDocsReadOnlyAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonWorkDocsReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 1 月 8 日 23:49 UTC
- 編集日時: 2020 年 1 月 8 日 23:49 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkDocsReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
        "ds:DescribeDirectories",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonWorkMailEventsServiceRolePolicy

説明: Amazon WorkMail Events が使用または管理する AWS のサービス および リソースへのアクセスを有効にします

`AmazonWorkMailEventsServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 4 月 16 日 16:52 UTC
- 編集日時: 2019 年 4 月 16 日 16:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonWorkMailEventsServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonWorkMailFullAccess

説明: WorkMail、Directory Service、SES、EC2 へのフルアクセスと KMS メタデータへの読み取りアクセスを提供します。

AmazonWorkMailFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonWorkMailFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2020 年 12 月 21 日 14:13 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkMailFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v10 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonWorkMailMessageFlowFullAccess

説明: WorkMail メッセージフロー API へのフルアクセス

AmazonWorkMailMessageFlowFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonWorkMailMessageFlowFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 2 月 11 日 11:08 UTC

- 編集日時: 2021 年 2 月 11 日 11:08 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkMailMessageFlowFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonWorkMailMessageFlowReadOnlyAccess

説明: GetRawMessageContent API の WorkMail メッセージへの読み取り専用アクセス

`AmazonWorkMailMessageFlowReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonWorkMailMessageFlowReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 1 月 28 日 12:40 UTC
- 編集日時: 2021 年 1 月 28 日 12:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkMailMessageFlowReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する

- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonWorkMailReadOnlyAccess

説明: WorkMail と SES への読み取り専用アクセスを提供します。

AmazonWorkMailReadOnlyAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonWorkMailReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2019 年 7 月 25 日 08:24 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkMailReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonWorkSpacesAdmin

説明: AWS SDK および CLI 経由で Amazon WorkSpaces 管理アクションへのアクセスを提供します。

AmazonWorkSpacesAdmin は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonWorkSpacesAdmin をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 9 月 22 日 22:21 UTC
- 編集日時: 2024 年 6 月 27 日 17:16 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonWorkSpacesAdmin",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListKeys",
        "workspaces:CreateTags",
        "workspaces:CreateWorkspaceImage",
        "workspaces:CreateWorkspaces",
        "workspaces:CreateWorkspacesPool",
        "workspaces:CreateStandbyWorkspaces",
        "workspaces:DeleteTags",
        "workspaces:DeregisterWorkspaceDirectory",
        "workspaces:DescribeTags",
        "workspaces:DescribeWorkspaceBundles",
        "workspaces:DescribeWorkspaceDirectories",
        "workspaces:DescribeWorkspaces",
        "workspaces:DescribeWorkspacesPools",
        "workspaces:DescribeWorkspacesPoolSessions",
        "workspaces:DescribeWorkspacesConnectionStatus",
        "workspaces:ModifyCertificateBasedAuthProperties",
        "workspaces:ModifySamlProperties",
        "workspaces:ModifyStreamingProperties",
        "workspaces:ModifyWorkspaceCreationProperties",
        "workspaces:ModifyWorkspaceProperties",
        "workspaces:RebootWorkspaces",
```

```
        "workspaces:RebuildWorkspaces",
        "workspaces:RegisterWorkspaceDirectory",
        "workspaces:RestoreWorkspace",
        "workspaces:StartWorkspaces",
        "workspaces:StartWorkspacesPool",
        "workspaces:StopWorkspaces",
        "workspaces:StopWorkspacesPool",
        "workspaces:TerminateWorkspaces",
        "workspaces:TerminateWorkspacesPool",
        "workspaces:TerminateWorkspacesPoolSession",
        "workspaces:UpdateWorkspacesPool"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonWorkSpacesApplicationManagerAdminAccess

説明: Amazon WorkSpaces アプリケーションマネージャーでアプリケーションをパッケージ化するための管理者アクセスを提供します。

AmazonWorkSpacesApplicationManagerAdminAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonWorkSpacesApplicationManagerAdminAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2015 年 4 月 9 日 14:03 UTC
- 編集日時: 2015 年 4 月 9 日 14:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesApplicationManagerAdminAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonWorkspacesPCAAccess

説明: この管理ポリシーは、証明書ベースの認証 AWS アカウント のために の AWS Certificate Manager プライベート CA リソースへの完全な管理アクセスを提供します。

AmazonWorkspacesPCAAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonWorkspacesPCAAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 11 月 8 日 00:25 UTC
- 編集日時: 2022 年 11 月 8 日 00:25 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkspacesPCAAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonWorkSpacesPoolServiceAccess

説明: このポリシーは、 AWS WorkSpaces Pools を起動するために必要なカスタマーアカウントリソースへの WorkSpaces サービスアクセスを提供します。

`AmazonWorkSpacesPoolServiceAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonWorkSpacesPoolServiceAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 6 月 27 日 16:21 UTC
- 編集日時: 2024 年 6 月 27 日 16:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesPoolServiceAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ProvisioningWorkSpacesPoolPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "WorkSpacesPoolS3Permissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:ListBucket",
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:GetObjectVersion",
        "s3:DeleteObjectVersion",
        "s3:GetBucketPolicy",
        "s3:PutBucketPolicy",
        "s3:PutEncryptionConfiguration"
      ],
      "Resource" : [
        "arn:aws:s3:::wspool-logs-*",
        "arn:aws:s3:::wspool-app-settings-*",
        "arn:aws:s3:::wspool-home-folder-*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonWorkSpacesSecureBrowserReadOnly

説明: Amazon WorkSpaces Secure Browser とその依存関係への読み取り専用アクセスを AWS マネジメントコンソール、、 SDK、および CLI 経由で提供します。

`AmazonWorkSpacesSecureBrowserReadOnly` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonWorkSpacesSecureBrowserReadOnly` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 6 月 24 日 20:01 UTC
- 編集日時: 2024 年 6 月 24 日 20:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesSecureBrowserReadOnly`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "WorkSpacesSecureBrowser",
      "Effect" : "Allow",
      "Action" : [
        "workspaces-web:GetBrowserSettings",
        "workspaces-web:GetIdentityProvider",
        "workspaces-web:GetNetworkSettings",
        "workspaces-web:GetPortal",
        "workspaces-web:GetPortalServiceProviderMetadata",
        "workspaces-web:GetTrustStore",
        "workspaces-web:GetTrustStoreCertificate",
        "workspaces-web:GetUserSettings",
        "workspaces-web:GetUserAccessLoggingSettings",
        "workspaces-web:GetIpAccessSettings",
        "workspaces-web:ListBrowserSettings",
        "workspaces-web:ListIdentityProviders",
        "workspaces-web:ListNetworkSettings",
        "workspaces-web:ListPortals",
        "workspaces-web:ListTagsForResource",
        "workspaces-web:ListTrustStoreCertificates",
        "workspaces-web:ListTrustStores",
        "workspaces-web:ListUserSettings",
        "workspaces-web:ListUserAccessLoggingSettings",
        "workspaces-web:ListIpAccessSettings"
      ],
      "Resource" : "arn:aws:workspaces-web:*:*:*"
    },
    {
      "Sid" : "Dependencies",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
```

```
        "kinesis:ListStreams"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonWorkSpacesSelfServiceAccess

説明: WorkSpace セルフサービスアクション実行のための Amazon WorkSpaces バックエンドサービスへのアクセスを提供します

`AmazonWorkSpacesSelfServiceAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonWorkSpacesSelfServiceAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 6 月 27 日 19:22 UTC
- 編集日時: 2019 年 6 月 27 日 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesSelfServiceAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonWorkSpacesServiceAccess

説明: AWS WorkSpaces を起動するための WorkSpaces サービスへのお客様のアカウントアクセスを提供します。

`AmazonWorkSpacesServiceAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonWorkSpacesServiceAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 6 月 27 日 19:19 UTC
- 編集日時: 2020 年 3 月 18 日 23:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesServiceAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonWorkSpacesThinClientFullAccess

説明: Amazon WorkSpaces シンクライアントへのフルアクセスと、必要な関連サービスへの制限付きアクセスを提供します

AmazonWorkSpacesThinClientFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonWorkSpacesThinClientFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 8 月 9 日 07:25 UTC
- 編集日時: 2025 年 8 月 26 日 17:34 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkSpacesThinClientFullAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
    {
      "Sid" : "AllowWorkSpacesAccess",
      "Effect" : "Allow",
      "Action" : [
        "workspaces:DescribeConnectionAliases",
        "workspaces:DescribeWorkspaceDirectories"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowWorkSpacesSecureBrowserAccess",
      "Effect" : "Allow",
      "Action" : [
        "workspaces-web:GetPortal",
        "workspaces-web:GetUserSettings",
        "workspaces-web:ListPortals"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAppStreamAccess",
      "Effect" : "Allow",
      "Action" : [
        "appstream:DescribeStacks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
monitoring.thinclient.amazonaws.com/
AWSServiceRoleForAmazonWorkSpacesThinClientMonitoring",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "monitoring.thinclient.amazonaws.com"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonWorkSpacesThinClientMonitoringServiceRolePolicy

説明: Amazon WorkSpaces シンクライアントモニタリングによって使用または管理される AWS のサービス および リソースへのアクセスを有効にします

`AmazonWorkSpacesThinClientMonitoringServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2025 年 6 月 13 日 19:37 UTC
- 編集日時: 2025 年 6 月 13 日 19:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonWorkSpacesThinClientMonitoringServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonWorkSpacesThinClientReadOnlyAccess

説明: Amazon WorkSpaces シンクライアントとその依存関係への読み取り専用アクセスを提供します

AmazonWorkSpacesThinClientReadOnlyAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonWorkSpacesThinClientReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 7 月 19 日 08:50 UTC
- 編集日時: 2025 年 1 月 9 日 16:52 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesThinClientReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowThinClientReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "thinclient:GetDevice",
        "thinclient:GetDeviceDetails",
        "thinclient:GetEnvironment",
        "thinclient:GetSoftwareSet",
        "thinclient:ListDevices",
        "thinclient:ListDeviceSessions",
        "thinclient:ListEnvironments",
        "thinclient:ListSoftwareSets",
        "thinclient:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowWorkSpacesAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "workspaces:DescribeConnectionAliases",
        "workspaces:DescribeWorkspaceDirectories"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowWorkSpacesSecureBrowserAccess",
      "Effect" : "Allow",
      "Action" : [
        "workspaces-web:GetPortal",
        "workspaces-web:GetUserSettings",
        "workspaces-web:ListPortals"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAppStreamAccess",
      "Effect" : "Allow",
      "Action" : [
        "appstream:DescribeStacks"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonWorkSpacesWebReadOnly

説明: Amazon WorkSpaces Web とその依存関係への読み取り専用アクセスを AWS マネジメントコンソール、、 SDK、および CLI 経由で提供します。

`AmazonWorkSpacesWebReadOnly` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonWorkSpacesWebReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 11 月 30 日 14:20 UTC
- 編集日時: 2022 年 11 月 2 日 20:20 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkSpacesWebReadOnly

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonWorkSpacesWebServiceRolePolicy

説明: Amazon WorkSpaces Web が使用または管理する AWS のサービス および リソースへのアクセスを有効にします

AmazonWorkSpacesWebServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 11 月 30 日 13:15 UTC
- 編集日時: 2022 年 12 月 15 日 22:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonWorkSpacesWebServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonZocaloFullAccess

説明: Amazon Zocalo へのフルアクセスを提供します。

AmazonZocaloFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonZocaloFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2015 年 2 月 6 日 18:41 UTC
- ARN: arn:aws:iam::aws:policy/AmazonZocaloFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmazonZocaloReadOnlyAccess

説明: Amazon Zocalo への読み取り専用アクセスを提供します

`AmazonZocaloReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonZocaloReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2015 年 2 月 6 日 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonZocaloReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "zocalo:Describe*",
        "ds:DescribeDirectories",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AmplifyBackendDeployFullAccess

説明: Development AWS クラウド Kit (AWS CDK) を介して Amplify バックエンドリソース (AWS AppSync、Amazon Cognito、Amazon S3、およびその他の関連サービス) をデプロイするためのフルアクセス許可を Amplify に提供します

`AmplifyBackendDeployFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmplifyBackendDeployFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 10 月 6 日 21:32 UTC
- 編集日時: 2024 年 11 月 14 日 19:09 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmplifyBackendDeployFullAccess

ポリシーのバージョン

ポリシーのバージョン: v9 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CDKPreDeploy",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:GetTemplate",
        "cloudformation:ListStackResources",
        "cloudformation:GetTemplateSummary",
        "cloudformation:DeleteStack"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/amplify-*",
        "arn:aws:cloudformation:*:*:stack/CDKToolkit/*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AmplifyMetadata",
      "Effect" : "Allow",
      "Action" : [
        "amplify:ListApps",
        "cloudformation:ListStacks",
        "ssm:DescribeParameters",
        "appsync:GetIntrospectionSchema",
        "amplify:GetBackendEnvironment"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AmplifyHotSwappableResources",
      "Effect" : "Allow",
      "Action" : [
        "appsync:GetSchemaCreationStatus",
        "appsync:StartSchemaCreation",
        "appsync:UpdateResolver",
        "appsync:ListFunctions",
        "appsync:UpdateFunction",
        "appsync:UpdateApiKey"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AmplifyHotSwappableFunctionResource",
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction",
        "lambda:UpdateFunctionCode",
        "lambda:GetFunction",
        "lambda:UpdateFunctionConfiguration"
      ],
      "Resource" : [
```

```
        "arn:aws:lambda:*:*:function:amplify-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AmplifySandboxLambdaLogsStreamingListTags",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListTags"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:amplify-*"
      ]
    },
    {
      "Sid" : "AmplifySandboxLambdaLogsStreamingFilterLogEvents",
      "Effect" : "Allow",
      "Action" : [
        "logs:FilterLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/lambda/amplify-*:*",
        "arn:aws:logs:*:*:log-group:amplify-*:*"
      ]
    },
    {
      "Sid" : "AmplifySchema",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*amplify*",
        "arn:aws:s3:::cdk-*-assets-*-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Sid" : "CDKDeploy",
      "Effect" : "Allow",
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/cdk-*-deploy-role-*-*",
        "arn:aws:iam::*:role/cdk-*-file-publishing-role-*-*",
        "arn:aws:iam::*:role/cdk-*-image-publishing-role-*-*",
        "arn:aws:iam::*:role/cdk-*-lookup-role-*-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AmplifySSM",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParametersByPath",
        "ssm:GetParameters",
        "ssm:GetParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/amplify/*",
        "arn:aws:ssm:*:*:parameter/cdk-bootstrap/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AmplifyModifySSMParam",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter",
        "ssm:DeleteParameter",
        "ssm:DeleteParameters"
```

```
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/amplify/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AmplifyDiscoverRDSVpcConfig",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBProxies",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "ec2:DescribeSubnets",
        "rds:DescribeDBSubnetGroups"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:db:*",
        "arn:aws:rds:*:*:cluster:*",
        "arn:aws:rds:*:*:db-proxy:*",
        "arn:aws:rds:*:*:subgrp:*",
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

APIGatewayServiceRolePolicy

説明: API Gateway が顧客に代わって関連する AWS リソースを管理できるようにします。

APIGatewayServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 10 月 20 日 17:23 UTC
- 編集日時: 2021 年 7 月 12 日 22:24 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/APIGatewayServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v9 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AppIntegrationsServiceLinkedRolePolicy

説明: AppIntegration がユーザーに代わって AppFlow リソースを管理し、CloudWatch メトリクスデータを公開することを許可します。

AppIntegrationsServiceLinkedRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 9 月 30 日 19:42 UTC
- 編集日時: 2022 年 9 月 30 日 19:42 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AppIntegrationsServiceLinkedRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

ApplicationAutoScalingForAmazonAppStreamAccess

説明: Amazon AppStream のアプリケーション自動スケーリングを有効にするポリシー

`ApplicationAutoScalingForAmazonAppStreamAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `ApplicationAutoScalingForAmazonAppStreamAccess` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2017 年 2 月 6 日 21:39 UTC
- 編集日時: 2017 年 2 月 6 日 21:39 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ApplicationAutoScalingForAmazonAppStreamAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appstream:UpdateFleet",
        "appstream:DescribeFleets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

ApplicationDiscoveryServiceContinuousExportServiceRolePolicy

説明: Application Discovery Service の継続的エクスポート機能によって使用または管理される AWS のサービス および リソースへのアクセスを有効にします

ApplicationDiscoveryServiceContinuousExportServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 8 月 9 日 20:22 UTC
- 編集日時: 2018 年 8 月 13 日 22:31 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/ApplicationDiscoveryServiceContinuousExportServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AppRunnerNetworkingServiceRolePolicy

説明: AWS AppRunner Networking がユーザーに代わって関連 AWS リソースを管理できるようにします。

AppRunnerNetworkingServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 1 月 12 日 21:02 UTC
- 編集日時: 2022 年 1 月 12 日 21:02 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AppRunnerNetworkingServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AppRunnerServiceRolePolicy

説明: AWS AppRunner がユーザーに代わって関連 AWS リソースを管理できるようにします。

AppRunnerServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 5 月 14 日 19:15 UTC
- 編集日時: 2021 年 5 月 14 日 19:15 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AppRunnerServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AppStudioServiceRolePolicy

説明: AppStudio がユーザーに代わって関連 AWS リソースを管理できるようにします。

AppStudioServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2024 年 7 月 10 日 05:01 UTC
- 編集日時: 2025 年 3 月 13 日 20:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AppStudioServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AppStudioResourcePermissionsForCloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/appstudio/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Sid" : "AppStudioResourcePermissionsForSecretsManager",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue",
        "secretsmanager:UpdateSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:appstudio-*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "IsAppStudioSecret"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/IsAppStudioSecret" : "true"
        }
      }
    },
    {
      "Sid" : "AppStudioResourcePermissionsForManagedSecrets",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue",
        "secretsmanager:UpdateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:appstudio!*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "appstudio"
        }
```

```
      }
    },
    {
      "Sid" : "AppStudioResourceWritePermissionsForManagedSecrets",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:appstudio!*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AppStudioResourcePermissionsForSSO",
      "Effect" : "Allow",
      "Action" : [
        "sso:GetManagedApplicationInstance",
        "sso-directory:DescribeUsers",
        "sso-directory:ListMembersInGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AuroraDsqlServiceLinkedRolePolicy

説明: Amazon Aurora DSQL のサービスにリンクされたロール用のポリシー

AuroraDsqlServiceLinkedRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2024 年 12 月 3 日 15:06 UTC
- 編集日時: 2025 年 5 月 9 日 19:22 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AuroraDsqlServiceLinkedRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
            "AWS/Usage"
          ],
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AutoScalingConsoleFullAccess

説明: 経由で Auto Scaling へのフルアクセスを提供します AWS マネジメントコンソール。

`AutoScalingConsoleFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AutoScalingConsoleFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 1 月 12 日 19:43 UTC
- 編集日時: 2018 年 2 月 6 日 23:15 UTC
- ARN: `arn:aws:iam::aws:policy/AutoScalingConsoleFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AutoScalingConsoleReadOnlyAccess

説明: 経由で Auto Scaling への読み取り専用アクセスを提供します AWS マネジメントコンソール。

AutoScalingConsoleReadOnlyAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AutoScalingConsoleReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 1 月 12 日 19:48 UTC
- 編集日時: 2017 年 1 月 12 日 19:48 UTC
- ARN: arn:aws:iam::aws:policy/AutoScalingConsoleReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AutoScalingFullAccess

説明: 自動スケーリングへのフルアクセスを提供します。

AutoScalingFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AutoScalingFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 1 月 12 日 19:31 UTC
- 編集日時: 2018 年 2 月 6 日 21:59 UTC
- ARN: arn:aws:iam::aws:policy/AutoScalingFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AutoScalingNotificationAccessRole

説明: AutoScaling 通知アクセスサービスロールのデフォルトのポリシーです。

AutoScalingNotificationAccessRole は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AutoScalingNotificationAccessRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2015 年 2 月 6 日 18:41 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AutoScalingNotificationAccessRole

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "sqs:SendMessage",
        "sqs:GetQueueUrl",
```

```
        "sns:Publish"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AutoScalingReadOnlyAccess

説明: 自動スケーリング への読み取り専用アクセスを提供します。

`AutoScalingReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AutoScalingReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 1 月 12 日 19:39 UTC
- 編集日時: 2017 年 1 月 12 日 19:39 UTC
- ARN: `arn:aws:iam::aws:policy/AutoScalingReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AutoScalingServiceRolePolicy

説明: Auto Scaling が使用または管理する AWS のサービス およびリソースへのアクセスを有効にします

AutoScalingServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 1 月 8 日 23:10 UTC
- 編集日時: 2025 年 11 月 12 日 18:19 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v10 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2InstanceManagement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachClassicLinkVpc",
        "ec2:CancelSpotInstanceRequests",
        "ec2:CreateReplaceRootVolumeTask",
        "ec2:CreateFleet",
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "ec2:Describe*",
        "ec2:DetachClassicLinkVpc",
        "ec2:GetInstanceTypesFromInstanceRequirements",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:ModifyInstanceAttribute",
        "ec2:RequestSpotInstances",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2InstanceProfileManagement",
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.amazonaws.com*"
        }
      }
    },
    {
      "Sid" : "EC2SpotManagement",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "spot.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ELBManagement",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:Register*",
        "elasticloadbalancing:Deregister*",
        "elasticloadbalancing:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CWManagement",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "SNSManagement",
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EventBridgeRuleManagement",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets",
        "events:DeleteRule"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SystemsManagerParameterManagement",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameters"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VpcLatticeManagement",
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:DeregisterTargets",
        "vpc-lattice:GetTargetGroup",
        "vpc-lattice:ListTargets",
        "vpc-lattice:ListTargetGroups",
        "vpc-lattice:RegisterTargets"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "ResourceGroupsManagement",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:ListGroupResources"
      ],
      "Resource" : "arn:*:resource-groups:*:*:group/*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWS-SSM-Automation-DiagnosisBucketPolicy

説明: SSM 診断 S3 バケットにアクセスして問題の診断と修復を行うためのアクセス許可を提供します。

AWS-SSM-Automation-DiagnosisBucketPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWS-SSM-Automation-DiagnosisBucketPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 11 月 15 日 23:31 UTC
- 編集日時: 2024 年 11 月 15 日 23:31 UTC
- ARN: arn:aws:iam::aws:policy/AWS-SSM-Automation-DiagnosisBucketPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadWriteToSsmDiagnosisBucketInSameAccount",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-diagnosis-*/actions/*/
${aws:PrincipalAccount}/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowReadWriteToSsmDiagnosisBucketWithinOrg",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-diagnosis-*/actions/*/
${aws:PrincipalAccount}/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceOrgId" : "${aws:PrincipalOrgId}"
        }
      }
    },
    {
      "Sid" : "AllowReadOnlyAccessListBucketOnSsmDiagnosisBucketInSameAccount",
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-diagnosis-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "s3:prefix" : "*/${aws:PrincipalAccount}/*"
        }
      }
    },
    {
      "Sid" : "AllowReadOnlyAccessListBucketOnSsmDiagnosisBucketWithinOrg",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-diagnosis-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceOrgId" : "${aws:PrincipalOrgId}"
        },
        "StringLike" : {
          "s3:prefix" : "*/${aws:PrincipalAccount}/*"
        }
      }
    },
    {
      "Sid" : "AllowGetEncryptionConfigurationOnSsmDiagnosisBucketInSameAccount",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetEncryptionConfiguration"
      ],
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-diagnosis-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
```

```
      "Sid" : "AllowGetEncryptionConfigurationOnSsmDiagnosisBucketWithinOrg",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetEncryptionConfiguration"
      ],
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-diagnosis-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceOrgId" : "${aws:PrincipalOrgId}"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy

説明: 自動化ドキュメント内で定義されたアクティビティを実行して SSM サービスの問題を診断するためのアクセス許可を付与します。これは主に、メンバーアカウント内で子オートメーションをトリガーしてクロスアカウントクロスリージョンのセットアップで自動化ドキュメントを実行するために使用されます。

`AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 11 月 16 日 00:01 UTC
- 編集日時: 2025 年 7 月 16 日 17:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadOnlyAccessSSMResource",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAutomationExecutions",
        "ssm:DescribeAutomationStepExecutions",
        "ssm:GetAutomationExecution"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowExecuteSSMAutomation",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-*UnmanagedEC2*",
        "arn:aws:ssm:*:*:automation-execution/*",
```

```
        "arn:aws:ssm:*:*:automation-definition/AWS-*UnmanagedEC2*:*"
      ]
    },
    {
      "Sid" : "AllowKMSOperations",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SystemsManagerManaged" : "true"
        },
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : "arn:aws:s3:::do-not-delete-ssm-
diagnosis-*"
        },
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "AllowAssumeDiagnosisExecutionRoleWithinAccount",
      "Effect" : "Allow",
      "Action" : "sts:AssumeRole",
      "Resource" : "arn:aws:iam::*:role/AWS-SSM-DiagnosisExecutionRole*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleOnSelfToSsm",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/AWS-SSM-DiagnosisAdminRole*",
      "Condition" : {
```

```
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowReadWriteToSsmDiagnosisBucketInSameAccount",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-diagnosis-*/actions/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowListBucketOnSsmDiagnosisBucketInSameAccount",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-diagnosis-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy

説明: 自動化ドキュメント内で定義されたアクティビティを実行して SSM サービスの問題を診断するためのアクセス許可を提供します。これは主に、すべてのノードで SSM サービスの正常性を診断することで、ターゲットアカウント/リージョンのセットアップで自動化ドキュメントを実行するために使用されます。

AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 11 月 16 日 00:08 UTC
- 編集日時: 2025 年 7 月 16 日 17:37 UTC
- ARN: arn:aws:iam::aws:policy/AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadOnlyAccessEC2Resource",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadOnlyAccessSSMResource",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAutomationStepExecutions",
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeAutomationExecutions",
        "ssm:GetAutomationExecution"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowExecuteSSMAutomation",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-*UnmanagedEC2*",
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:automation-definition/AWS-*UnmanagedEC2*:*"
      ]
    },
    {
      "Sid" : "AllowKMSOperations",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SystemsManagerManaged" : "true"
```

```
        },
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : "arn:aws:s3:::do-not-delete-ssm-
diagnosis-*"
        },
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleOnSelfToSsm",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/AWS-SSM-DiagnosisExecutionRole*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrationRolePolicy

説明: SSM オートメーションに必要な組織固有のアクセス許可を提供して、運用アカウントが非マネージドノードを診断するためのアクセス許可を提供します。これにより、組織のルート内のメン

バーアカウントのリストを取得して、ターゲットアカウント/リージョンで実行ロールを引き受け、クロスアカウントクロスリージョン実行をトリガーできます。

AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrationRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrationRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 11 月 16 日 00:11 UTC
- 編集日時: 2024 年 11 月 16 日 00:11 UTC
- ARN: arn:aws:iam::aws:policy/AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrationRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadOnlyAccessOrganization",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListRoots",
        "organizations:ListChildren"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAssumeDiagnosisExecutionRoleWithinOrg",
      "Effect" : "Allow",
      "Action" : "sts:AssumeRole",
      "Resource" : "arn:aws:iam::*:role/AWS-SSM-DiagnosisExecutionRole*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceOrgId" : "${aws:PrincipalOrgId}"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWS-SSM-RemediationAutomation-AdministrationRolePolicy

説明: 自動化ドキュメント内で定義されたアクティビティを実行して SSM サービスの問題を修復するためのアクセス許可を提供します。これは主に、メンバーアカウント内で子オートメーションをトリガーしてクロスアカウントクロスリージョンのセットアップで自動化ドキュメントを実行するために使用されます。

AWS-SSM-RemediationAutomation-AdministrationRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWS-SSM-RemediationAutomation-AdministrationRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 11 月 16 日 00:14 UTC
- 編集日時: 2025 年 7 月 16 日 17:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWS-SSM-RemediationAutomation-AdministrationRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadOnlyAccessSSMResource",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAutomationExecutions",
        "ssm:DescribeAutomationStepExecutions",
        "ssm:GetAutomationExecution"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowExecuteSSMAutomation",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-OrchestrateUnmanagedEC2Actions",
        "arn:aws:ssm:*:*:document/AWS-RemediateSSMAgent*",
```

```
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:automation-definition/AWS-OrchestrateUnmanagedEC2Actions:*",
        "arn:aws:ssm:*:*:automation-definition/AWS-RemediateSSMAgent*:*"
      ]
    },
    {
      "Sid" : "AllowKMSOperations",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SystemsManagerManaged" : "true"
        },
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : "arn:aws:s3:::do-not-delete-ssm-
diagnosis-*"
        },
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "AllowAssumeRemediationExecutionRoleWithinAccount",
      "Effect" : "Allow",
      "Action" : "sts:AssumeRole",
      "Resource" : "arn:aws:iam::*:role/AWS-SSM-RemediationExecutionRole*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleOnSelfToSsm",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
```

```
      "Resource" : "arn:aws:iam::*:role/AWS-SSM-RemediationAdminRole*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowReadWriteToSsmDiagnosisBucketInSameAccount",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-diagnosis-*/actions/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowListBucketOnSsmDiagnosisBucketInSameAccount",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-diagnosis-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWS-SSM-RemediationAutomation-ExecutionRolePolicy

説明: 自動化ドキュメント内で定義されたアクティビティを実行して SSM サービスの問題を修復するためのアクセス許可を提供します。これは主に、すべてのノードで SSM サービスの正常性を修復することで、ターゲットアカウント/リージョンのセットアップで自動化ドキュメントを実行するために使用されます。

AWS-SSM-RemediationAutomation-ExecutionRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWS-SSM-RemediationAutomation-ExecutionRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 11 月 16 日 00:17 UTC
- 編集日時: 2025 年 7 月 16 日 19:07 UTC
- ARN: arn:aws:iam::aws:policy/AWS-SSM-RemediationAutomation-ExecutionRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
  "Statement" : [
    {
      "Sid" : "AllowReadOnlyAccessSSMResource",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution",
        "ssm:DescribeAutomationExecutions",
        "ssm:DescribeAutomationStepExecutions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadOnlyAccessEC2Resource",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCreateVpcEndpointForTaggedSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SystemsManager::FindingNetworkingSecurityGroups::VPCE::SG" :
"VPCEndpointSecurityGroup"
        }
      }
    },
    {
      "Sid" : "AllowCreateVpcEndpoint",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
```

```
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Sid" : "RestrictCreateVpcEndpointForSSMService",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:VpceServiceName" : [
            "com.amazonaws.*.ssm",
            "com.amazonaws.*.ssmmessages",
            "com.amazonaws.*.ec2messages"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/SystemsManager::FindingNetworkingVPCEndpoints::VPCE" :
"VPCEndpoint"
        }
      }
    },
    {
      "Sid" : "RestrictCreateVpcEndpointWithTag",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SystemsManager::FindingNetworkingVPCEndpoints::VPCE" :
"VPCEndpoint",
          "ec2:CreateAction" : [
            "CreateVpcEndpoint"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "AllowModifyVpcAttributeForDns",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:Attribute" : [
            "EnableDnsSupport",
            "EnableDnsHostnames"
          ]
        }
      }
    },
    {
      "Sid" : "AllowSecurityGroupRuleUpdate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "AllowSecurityGroupRuleUpdateForTaggedResource",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SystemsManager::FindingNetworkingSecurityGroups::VPCE::SG" :
"VPCEndpointSecurityGroup"
```

```
        }
      }
    },
    {
      "Sid" : "AllowSecurityGroupRuleUpdateWithTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group-rule/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SystemsManager::FindingNetworkingSecurityGroups::SG::Rule" :
"HTTPSAccess"
        }
      }
    },
    {
      "Sid" : "AllowSecurityGroupRuleUpdateTagRule",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group-rule/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SystemsManager::FindingNetworkingSecurityGroups::SG::Rule" :
"HTTPSAccess",
          "ec2:CreateAction" : [
            "AuthorizeSecurityGroupEgress",
            "AuthorizeSecurityGroupIngress"
          ]
        }
      }
    },
    {
      "Sid" : "AllowCreateSecurityGroupForVPCEndpoint",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
```

```
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "AllowCreateSecurityGroupWithTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SystemsManager::FindingNetworkingSecurityGroups::VPCE::SG" :
"VPCEndpointSecurityGroup"
        }
      }
    },
    {
      "Sid" : "AllowTagCreationForSecurityGroupTags",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SystemsManager::FindingNetworkingSecurityGroups::VPCE::SG" :
"VPCEndpointSecurityGroup",
          "ec2:CreateAction" : [
            "CreateSecurityGroup"
          ]
        }
      }
    },
    {
      "Sid" : "AllowExecuteSSMAutomation",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
```

```
        "arn:aws:ssm:*:*:document/AWS-OrchestrateUnmanagedEC2Actions",
        "arn:aws:ssm:*:*:document/AWS-RemediateSSMAgent*",
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:automation-definition/AWS-OrchestrateUnmanagedEC2Actions:*",
        "arn:aws:ssm:*:*:automation-definition/AWS-RemediateSSMAgent*:*"
      ]
    },
    {
      "Sid" : "AllowKMSOperations",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SystemsManagerManaged" : "true"
        },
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : "arn:aws:s3:::do-not-delete-ssm-
diagnosis-*"
        },
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleOnSelfToSsm",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/AWS-SSM-RemediationExecutionRole*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      }
    }
  ]
```

```
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWS-SSM-RemediationAutomation-OperationalAccountAdministrationRolePolicy

説明: SSM オートメーションに必要な組織固有のアクセス許可を提供して、運用アカウントが非マネージドノードを修復するためのアクセス許可を提供します。これにより、組織のルート内のメンバーアカウントのリストを取得して、ターゲットアカウント/リージョンで実行ロールを引き受け、クロスアカウントクロスリージョン実行をトリガーできます。

`AWS-SSM-RemediationAutomation-OperationalAccountAdministrationRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWS-SSM-RemediationAutomation-OperationalAccountAdministrationRolePolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 11 月 16 日 00:25 UTC
- 編集日時: 2024 年 11 月 16 日 00:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWS-SSM-RemediationAutomation-OperationalAccountAdministrationRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadOnlyAccessOrganization",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListRoots",
        "organizations:ListChildren"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAssumeRemediationExecutionRoleWithinOrg",
      "Effect" : "Allow",
      "Action" : "sts:AssumeRole",
      "Resource" : "arn:aws:iam::*:role/AWS-SSM-RemediationExecutionRole*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceOrgId" : "${aws:PrincipalOrgId}"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWS_ConfigRole

説明: Config AWS サービスロールのデフォルトポリシー。Config AWS が AWS リソースの変更を追跡するために必要なアクセス許可を提供します。

AWS_ConfigRole は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWS_ConfigRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 9 月 15 日 20:30 UTC
- 編集日時: 2025 年 11 月 21 日 17:04 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWS_ConfigRole

ポリシーのバージョン

ポリシーのバージョン: v42 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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:GetAccountConfiguration",
        "acm:ListCertificates",
        "acm:ListTagsForCertificate",
        "airflow:GetEnvironment",
        "airflow:ListEnvironments",
        "airflow:ListTagsForResource",
        "amplify:GetApp",
        "amplify:GetBranch",
        "amplify:GetDomainAssociation",
        "amplify:ListApps",
        "amplify:ListBranches",
        "amplify:ListDomainAssociations",
        "amplify:ListTagsForResource",
        "amplifyuibuilder:ExportThemes",
        "amplifyuibuilder:GetTheme",
        "amplifyuibuilder:ListForms",
        "amplifyuibuilder:ListThemes",
        "aoss:BatchGetCollection",
        "aoss:BatchGetLifecyclePolicy",
        "aoss:BatchGetVpcEndpoint",
        "aoss:GetAccessPolicy",
        "aoss:GetSecurityConfig",
        "aoss:GetSecurityPolicy",
        "aoss:ListAccessPolicies",
        "aoss:ListCollections",
        "aoss:ListLifecyclePolicies",
        "aoss:ListSecurityConfigs",
        "aoss:ListSecurityPolicies",
        "aoss:ListVpcEndpoints",
        "apigateway:GET",
        "app-integrations:GetApplication",
        "app-integrations:GetDataIntegration",
        "app-integrations:GetEventIntegration",
        "app-integrations:ListApplications",
        "app-integrations:ListDataIntegrations",
        "app-integrations:ListEventIntegrationAssociations",
        "app-integrations:ListEventIntegrations",
```

```
        "app-integrations:ListTagsForResource",
        "appconfig:GetApplication",
        "appconfig:GetConfigurationProfile",
        "appconfig:GetDeployment",
        "appconfig:GetDeploymentStrategy",
        "appconfig:GetEnvironment",
        "appconfig:GetExtension",
        "appconfig:GetExtensionAssociation",
        "appconfig:GetHostedConfigurationVersion",
        "appconfig:ListApplications",
        "appconfig:ListConfigurationProfiles",
        "appconfig:ListDeployments",
        "appconfig:ListDeploymentStrategies",
        "appconfig:ListEnvironments",
        "appconfig:ListExtensionAssociations",
        "appconfig:ListExtensions",
        "appconfig:ListHostedConfigurationVersions",
        "appconfig:ListTagsForResource",
        "appflow:DescribeConnectorProfiles",
        "appflow:DescribeFlow",
        "appflow:ListFlows",
        "appflow:ListTagsForResource",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "application-signals:GetServiceLevelObjective",
        "application-signals:ListServiceLevelObjectives",
        "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:DescribeObservabilityConfiguration",
        "apprunner:DescribeService",
        "apprunner:DescribeVpcConnector",
```

```
        "apprunner:DescribeVpcIngressConnection",
        "apprunner:ListObservabilityConfigurations",
        "apprunner:ListServices",
        "apprunner:ListTagsForResource",
        "apprunner:ListVpcConnectors",
        "appstream:DescribeAppBlockBuilders",
        "appstream:DescribeApplications",
        "appstream:DescribeDirectoryConfigs",
        "appstream:DescribeFleets",
        "appstream:DescribeStacks",
        "appstream:ListTagsForResource",
        "appsync:GetApiCache",
        "appsync:GetGraphqlApi",
        "appsync:GetSourceApiAssociation",
        "appsync:ListGraphqlApis",
        "appsync:ListSourceApiAssociations",
        "aps:DescribeAlertManagerDefinition",
        "aps:DescribeLoggingConfiguration",
        "APS:DescribeRuleGroupsNamespace",
        "APS:DescribeWorkspace",
        "aps:ListRuleGroupsNamespaces",
        "aps:ListTagsForResource",
        "APS:ListWorkspaces",
        "application-signals:ListServiceLevelObjectiveExclusionWindows",
        "application-signals:ListTagsForResource",
        "apprunner:DescribeAutoScalingConfiguration",
        "apprunner:ListAutoScalingConfigurations",
        "apprunner:ListVpcIngressConnections",
        "appstream:DescribeAppBlocks",
        "appstream:DescribeImageBuilders",
        "appsync:GetApi",
        "appsync:GetDomainName",
        "appsync:ListApis",
        "appsync:ListDomainNames",
        "appsync:ListTagsForResource",
        "apptest:GetTestCase",
        "apptest:ListTagsForResource",
        "apptest:ListTestCases",
        "aps:DescribeScraper",
        "aps:DescribeScraperLoggingConfiguration",
        "aps:ListScrapers",
        "arc-zonal-shift:GetAutoshiftObserverNotificationStatus",
        "athena:GetDataCatalog",
        "athena:GetPreparedStatement",
```

```
        "athena:GetWorkGroup",
        "athena:ListDataCatalogs",
        "athena:ListPreparedStatements",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups",
        "auditmanager:GetAccountStatus",
        "auditmanager:GetAssessment",
        "auditmanager:ListAssessments",
        "autoscaling-plans:DescribeScalingPlanResources",
        "autoscaling-plans:DescribeScalingPlans",
        "autoscaling-plans:GetScalingPlanResourceForecastData",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeLaunchConfigurations",
        "autoscaling:DescribeLifecycleHooks",
        "autoscaling:DescribePolicies",
        "autoscaling:DescribeScheduledActions",
        "autoscaling:DescribeTags",
        "autoscaling:DescribeWarmPool",
        "b2bi:GetCapability",
        "b2bi:GetPartnership",
        "b2bi:GetProfile",
        "b2bi:GetTransformer",
        "b2bi:ListCapabilities",
        "b2bi:ListPartnerships",
        "b2bi:ListProfiles",
        "b2bi:ListTagsForResource",
        "b2bi:ListTransformers",
        "backup-gateway:GetHypervisor",
        "backup-gateway:ListHypervisors",
        "backup-gateway:ListTagsForResource",
        "backup-gateway:ListVirtualMachines",
        "backup:DescribeBackupVault",
        "backup:DescribeFramework",
        "backup:DescribeProtectedResource",
        "backup:DescribeRecoveryPoint",
        "backup:DescribeReportPlan",
        "backup:GetBackupPlan",
        "backup:GetBackupSelection",
        "backup:GetBackupVaultAccessPolicy",
        "backup:GetBackupVaultNotifications",
        "backup:GetRestoreTestingPlan",
        "backup:GetRestoreTestingSelection",
        "backup:ListBackupPlans",
        "backup:ListBackupSelections",
```

```
        "backup:ListBackupVaults",
        "backup:ListFrameworks",
        "backup:ListRecoveryPointsByBackupVault",
        "backup:ListReportPlans",
        "backup:ListRestoreTestingPlans",
        "backup:ListRestoreTestingSelections",
        "backup:ListTags",
        "batch:DescribeComputeEnvironments",
        "batch:DescribeJobQueues",
        "batch:DescribeSchedulingPolicies",
        "batch:ListSchedulingPolicies",
        "batch:ListTagsForResource",
        "bcm-data-exports:GetExport",
        "bcm-data-exports:ListExports",
        "bcm-data-exports:ListTagsForResource",
        "bedrock-agentcore:GetAgentRuntime",
        "bedrock-agentcore:GetAgentRuntimeEndpoint",
        "bedrock-agentcore:GetBrowser",
        "bedrock-agentcore:GetCodeInterpreter",
        "bedrock-agentcore:ListAgentRuntimeEndpoints",
        "bedrock-agentcore:ListAgentRuntimes",
        "bedrock-agentcore:ListBrowsers",
        "bedrock-agentcore:ListCodeInterpreters",
        "bedrock-agentcore:ListTagsForResource",
        "bedrock:GetAgent",
        "bedrock:GetAgentActionGroup",
        "bedrock:GetAgentAlias",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:GetDataAutomationProject",
        "bedrock:GetDataSource",
        "bedrock:GetFlow",
        "bedrock:GetFlowAlias",
        "bedrock:GetFlowVersion",
        "bedrock:GetGuardrail",
        "bedrock:GetInferenceProfile",
        "bedrock:GetKnowledgeBase",
        "bedrock:GetModelInvocationLoggingConfiguration",
        "bedrock:ListAgentActionGroups",
        "bedrock:ListAgentAliases",
        "bedrock:ListAgentCollaborators",
        "bedrock:ListAgentKnowledgeBases",
        "bedrock:ListAgents",
        "bedrock:ListDataAutomationProjects",
        "bedrock:ListDataSources",
```

```
        "bedrock:ListFlowAliases",
        "bedrock:ListFlowVersions",
        "bedrock:ListFlows",
        "bedrock:ListGuardrails",
        "bedrock:ListInferenceProfiles",
        "bedrock:ListKnowledgeBases",
        "bedrock:ListPrompts",
        "bedrock:ListTagsForResource",
        "billingconductor:ListAccountAssociations",
        "billingconductor:ListBillingGroups",
        "billingconductor:ListCustomLineItems",
        "billingconductor:ListPricingPlans",
        "billingconductor:ListPricingRules",
        "billingconductor:ListPricingRulesAssociatedToPricingPlan",
        "billingconductor:ListTagsForResource",
        "budgets:DescribeBudgetAction",
        "budgets:DescribeBudgetActionsForAccount",
        "budgets:DescribeBudgetActionsForBudget",
        "budgets:ViewBudget",
        "cassandra:Select",
        "ce:DescribeCostCategoryDefinition",
        "ce:GetAnomalyMonitors",
        "ce:GetAnomalySubscriptions",
        "ce:ListCostCategoryDefinitions",
        "ce:ListTagsForResource",
        "cleanrooms-ml:GetTrainingDataset",
        "cleanrooms-ml:ListTrainingDatasets",
        "cleanrooms:GetAnalysisTemplate",
        "cleanrooms:GetConfiguredTable",
        "cleanrooms:GetConfiguredTableAnalysisRule",
        "cleanrooms:GetMembership",
        "cleanrooms:GetPrivacyBudgetTemplate",
        "cleanrooms:ListAnalysisTemplates",
        "cleanrooms:ListConfiguredTables",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListPrivacyBudgetTemplates",
        "cleanrooms:ListTagsForResource",
        "cloud9:DescribeEnvironmentMemberships",
        "cloud9:DescribeEnvironments",
        "cloud9:ListEnvironments",
        "cloud9:ListTagsForResource",
        "cloudformation:BatchDescribeTypeConfigurations",
        "cloudformation:DescribePublisher",
        "cloudformation:DescribeStackInstance",
```

```
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeType",
        "cloudformation:GetResource",
        "cloudformation:ListResources",
        "cloudformation:ListStackInstances",
        "cloudformation:ListStackResources",
        "cloudformation:ListStacks",
        "cloudformation:ListStackSets",
        "cloudformation:ListTypes",
        "cloudfront:DescribeFunction",
        "cloudfront:DescribeKeyValueStore",
        "cloudfront:GetFunction",
        "cloudfront:GetOriginAccessControl",
        "cloudfront:GetPublicKey",
        "cloudfront:GetRealtimeLogConfig",
        "cloudfront:GetResponseHeadersPolicy",
        "cloudfront:ListDistributions",
        "cloudfront:ListFunctions",
        "cloudfront:ListOriginAccessControls",
        "cloudfront:ListPublicKeys",
        "cloudfront:ListRealtimeLogConfigs",
        "cloudfront:ListResponseHeadersPolicies",
        "cloudfront:ListTagsForResource",
        "cloudtrail:DescribeTrails",
        "cloudTrail:GetChannel",
        "cloudtrail:GetEventConfiguration",
        "cloudtrail:GetEventDataStore",
        "cloudtrail:GetEventSelectors",
        "cloudtrail:GetInsightSelectors",
        "cloudtrail:GetResourcePolicy",
        "cloudtrail:GetTrailStatus",
        "cloudTrail:ListChannels",
        "cloudfront:GetConnectionGroup",
        "cloudfront:GetDistributionTenant",
        "cloudfront:GetVpcOrigin",
        "cloudfront:ListConnectionGroups",
        "cloudfront:ListDistributionTenants",
        "cloudfront:ListKeyValueStores",
        "cloudfront:ListVpcOrigins",
        "cloudtrail:GetDashboard",
        "cloudtrail:ListDashboards",
        "cloudtrail:ListEventDataStores",
        "cloudtrail:ListTags",
        "cloudtrail:ListTrails",
```

```
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:DescribeAnomalyDetectors",
        "cloudwatch:GetDashboard",
        "cloudwatch:GetMetricStream",
        "cloudwatch:ListDashboards",
        "cloudwatch:ListMetricStreams",
        "cloudwatch:ListTagsForResource",
        "codeartifact:DescribeDomain",
        "codeartifact:DescribePackageGroup",
        "codeartifact:DescribeRepository",
        "codeartifact:GetDomainPermissionsPolicy",
        "codeartifact:GetRepositoryPermissionsPolicy",
        "codeartifact:ListAllowedRepositoriesForGroup",
        "codeartifact:ListDomains",
        "codeartifact:ListPackageGroups",
        "codeartifact:ListPackages",
        "codeartifact:ListPackageVersions",
        "codeartifact:ListRepositories",
        "codeartifact:ListTagsForResource",
        "codebuild:BatchGetReportGroups",
        "codebuild:ListReportGroups",
        "codecommit:GetRepository",
        "codecommit:GetRepositoryTriggers",
        "codecommit:ListRepositories",
        "codecommit:ListTagsForResource",
        "codeconnections:GetConnection",
        "codeconnections:ListConnections",
        "codeconnections:ListTagsForResource",
        "codedeploy:GetDeploymentConfig",
        "codeguru-profiler:DescribeProfilingGroup",
        "codeguru-profiler:GetNotificationConfiguration",
        "codeguru-profiler:GetPolicy",
        "codeguru-profiler:ListProfilingGroups",
        "codeguru-reviewer:DescribeRepositoryAssociation",
        "codeguru-reviewer:ListRepositoryAssociations",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:ListActionTypes",
        "codepipeline:ListPipelines",
        "codepipeline:ListTagsForResource",
        "codepipeline:ListWebhooks",
        "codestar-connections:GetConnection",
        "codestar-connections:GetRepositoryLink",
```

```
        "codestar-connections:ListConnections",
        "codestar-connections:ListRepositoryLinks",
        "codestar-connections:ListTagsForResource",
        "cognito-identity:DescribeIdentityPool",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:GetPrincipalTagAttributeMap",
        "cognito-identity:ListIdentityPools",
        "cognito-identity:ListTagsForResource",
        "cognito-idp: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",
        "comprehend:DescribeFlywheel",
        "comprehend:ListFlywheels",
        "comprehend:ListTagsForResource",
        "config:BatchGet*",
        "config:Describe*",
        "config:Get*",
        "config:List*",
        "config:Put*",
        "config:Select*",
        "connect:DescribeEvaluationForm",
        "connect:DescribeInstance",
        "connect:DescribeInstanceStorageConfig",
        "connect:DescribePhoneNumber",
        "connect:DescribePredefinedAttribute",
        "connect:DescribePrompt",
        "connect:DescribeQueue",
        "connect:DescribeQuickConnect",
        "connect:DescribeRoutingProfile",
        "connect:DescribeRule",
        "connect:DescribeSecurityProfile",
        "connect:DescribeTrafficDistributionGroup",
        "connect:DescribeUser",
        "connect:DescribeView",
```

```
        "connect:GetTaskTemplate",
        "connect:ListApprovedOrigins",
        "connect:ListEvaluationForms",
        "connect:ListInstanceAttributes",
        "connect:ListInstances",
        "connect:ListInstanceStorageConfigs",
        "connect:ListIntegrationAssociations",
        "connect:ListPhoneNumbers",
        "connect:ListPhoneNumbersV2",
        "connect:ListPredefinedAttributes",
        "connect:ListPrompts",
        "connect:ListQueueQuickConnects",
        "connect:ListQueues",
        "connect:ListQuickConnects",
        "connect:ListRoutingProfileQueues",
        "connect:ListRoutingProfiles",
        "connect:ListRules",
        "connect:ListSecurityKeys",
        "connect:ListSecurityProfileApplications",
        "connect:ListSecurityProfilePermissions",
        "connect:ListSecurityProfiles",
        "connect:ListTagsForResource",
        "connect:ListTaskTemplates",
        "connect:ListTrafficDistributionGroups",
        "connect:ListUsers",
        "connect:ListViewVersions",
        "connect:ListViews",
        "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",
        "datazone:GetDomain",
        "datazone:ListDomains",
        "dax:DescribeClusters",
        "dax:DescribeParameterGroups",
        "dax:DescribeParameters",
        "dax:DescribeSubnetGroups",
        "dax:ListTags",
        "deadline:GetFarm",
        "deadline:GetFleet",
        "deadline:GetMonitor",
        "deadline:GetQueueFleetAssociation",
        "deadline:ListFarms",
        "deadline:ListFleets",
        "deadline:ListMonitors",
        "deadline:ListQueueFleetAssociations",
        "deadline:ListTagsForResource",
        "detective:ListGraphs",
        "detective:ListOrganizationAdminAccount",
        "detective:ListTagsForResource",
        "devicefarm:GetInstanceProfile",
        "devicefarm:GetNetworkProfile",
        "devicefarm:GetProject",
        "devicefarm:GetTestGridProject",
        "devicefarm:ListInstanceProfiles",
        "devicefarm:ListNetworkProfiles",
        "devicefarm:ListProjects",
        "devicefarm:ListTagsForResource",
        "devicefarm:ListTestGridProjects",
        "devops-guru:GetResourceCollection",
        "devops-guru:ListNotificationChannels",
        "directconnect:DescribeConnections",
        "dms:DescribeCertificates",
        "dms:DescribeDataMigrations",
```

```
            "dms:DescribeEndpoints",
            "dms:DescribeEventSubscriptions",
            "dms:DescribeReplicationConfigs",
            "dms:DescribeReplicationInstances",
            "dms:DescribeReplicationSubnetGroups",
            "dms:DescribeReplicationTaskAssessmentRuns",
            "dms:DescribeReplicationTasks",
            "dms:ListMigrationProjects",
            "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:GetAllowedImagesSettings",
            "ec2:GetEbsEncryptionByDefault",
            "ec2:GetInstanceTypesFromInstanceRequirements",
            "ec2:GetIpamPoolAllocations",
            "ec2:GetIpamPoolCidrs",
            "ec2:GetManagedPrefixListEntries",
            "ec2:GetNetworkInsightsAccessScopeAnalysisFindings",
            "ec2:GetNetworkInsightsAccessScopeContent",
            "ec2:GetSnapshotBlockPublicAccessState",
            "ec2:GetTransitGatewayRouteTablePropagations",
            "ec2:GetVerifiedAccessGroupPolicy",
            "ec2:SearchLocalGatewayRoutes",
            "ec2:SearchTransitGatewayMulticastGroups",
            "ecr-public:DescribeRepositories",
            "ecr-public:GetRepositoryCatalogData",
            "ecr-public:GetRepositoryPolicy",
            "ecr-public:ListTagsForResource",
            "ecr:BatchGetRepositoryScanningConfiguration",
            "ecr:DescribePullThroughCacheRules",
            "ecr:DescribeRegistry",
```

```
        "ecr:DescribeRepositories",
        "ecr:DescribeRepositoryCreationTemplates",
        "ecr:GetLifecyclePolicy",
        "ecr:GetRegistryPolicy",
        "ecr:GetRepositoryPolicy",
        "ecr:ListTagsForResource",
        "ecs:DescribeCapacityProviders",
        "ecs:DescribeClusters",
        "ecs:DescribeServices",
        "ecs:DescribeTaskDefinition",
        "ecs:DescribeTaskSets",
        "ecs:ListClusters",
        "ecs:ListServices",
        "ecs:ListTagsForResource",
        "ecs:ListTaskDefinitionFamilies",
        "ecs:ListTaskDefinitions",
        "eks:DescribeAccessEntry",
        "eks:DescribeAddon",
        "eks:DescribeCluster",
        "eks:DescribeFargateProfile",
        "eks:DescribeIdentityProviderConfig",
        "eks:DescribeNodegroup",
        "eks:DescribePodIdentityAssociation",
        "eks:ListAccessEntries",
        "eks:ListAddons",
        "eks:ListAssociatedAccessPolicies",
        "eks:ListClusters",
        "eks:ListFargateProfiles",
        "eks:ListIdentityProviderConfigs",
        "eks:ListNodegroups",
        "eks:ListPodIdentityAssociations",
        "eks:ListTagsForResource",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeCacheParameterGroups",
        "elasticache:DescribeCacheParameters",
        "elasticache:DescribeCacheSecurityGroups",
        "elasticache:DescribeCacheSubnetGroups",
        "elasticache:DescribeGlobalReplicationGroups",
        "elasticache:DescribeReplicationGroups",
        "elasticache:DescribeSnapshots",
        "elasticache:DescribeUserGroups",
        "elasticache:DescribeUsers",
        "elasticache:ListTagsForResource",
        "elasticbeanstalk:DescribeConfigurationSettings",
```

```
        "elasticbeanstalk:DescribeEnvironments",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeBackupPolicy",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeMountTargetSecurityGroups",
        "elasticfilesystem:DescribeTags",
        "elasticloadbalancing:DescribeListenerCertificates",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancerPolicies",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:DescribeSecurityConfiguration",
        "elasticmapreduce:DescribeStep",
        "elasticmapreduce:DescribeStudio",
        "elasticmapreduce:GetAutoTerminationPolicy",
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:GetManagedScalingPolicy",
        "elasticmapreduce:GetStudioSessionMapping",
        "elasticmapreduce:ListBootstrapActions",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListInstanceFleets",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListSecurityConfigurations",
        "elasticmapreduce:ListSteps",
        "elasticmapreduce:ListStudios",
        "elasticmapreduce:ListStudioSessionMappings",
        "emr-containers:DescribeJobRun",
        "emr-containers:DescribeVirtualCluster",
        "emr-containers:ListJobRuns",
        "emr-containers:ListManagedEndpoints",
        "emr-containers:ListVirtualClusters",
        "emr-serverless:GetApplication",
        "emr-serverless:GetJobRun",
        "emr-serverless:ListApplications",
```

```
        "emr-serverless:ListJobRuns",
        "entityresolution:GetIdMappingWorkflow",
        "entityresolution:GetMatchingWorkflow",
        "entityresolution:GetSchemaMapping",
        "entityresolution:ListIdMappingWorkflows",
        "entityresolution:ListMatchingWorkflows",
        "entityresolution:ListSchemaMappings",
        "entityresolution:ListTagsForResource",
        "es:DescribeDomain",
        "es:DescribeDomains",
        "es:DescribeElasticsearchDomain",
        "es:DescribeElasticsearchDomains",
        "es:GetCompatibleElasticsearchVersions",
        "es:GetCompatibleVersions",
        "es:ListDomainNames",
        "es:ListTags",
        "events:DescribeApiDestination",
        "events:DescribeArchive",
        "events:DescribeConnection",
        "events:DescribeEndpoint",
        "events:DescribeEventBus",
        "events:DescribeRule",
        "events:ListApiDestinations",
        "events:ListArchives",
        "events:ListConnections",
        "events:ListEndpoints",
        "events:ListEventBuses",
        "events:ListRules",
        "events:ListTagsForResource",
        "events:ListTargetsByRule",
        "evidently:GetLaunch",
        "evidently:GetProject",
        "evidently:GetSegment",
        "evidently:ListLaunches",
        "evidently:ListProjects",
        "evidently:ListSegments",
        "evidently:ListTagsForResource",
        "finspace:GetEnvironment",
        "finspace:ListEnvironments",
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams",
        "firehose:ListTagsForDeliveryStream",
        "fis:GetExperimentTemplate",
        "fis: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:DescribeContainerGroupDefinition",
        "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:ListContainerGroupDefinitions",
        "gamelift:ListFleets",
        "gamelift:ListGameServerGroups",
        "gamelift:ListScripts",
        "gamelift:ListTagsForResource",
        "geo:DescribeGeofenceCollection",
        "geo:DescribeKey",
        "geo:DescribeMap",
        "geo:DescribePlaceIndex",
        "geo:DescribeRouteCalculator",
        "geo:DescribeTracker",
        "geo:ListGeofenceCollections",
        "geo:ListKeys",
        "geo:ListMaps",
        "geo:ListPlaceIndexes",
        "geo:ListRouteCalculators",
        "geo:ListTrackerConsumers",
        "geo:ListTrackers",
        "globalaccelerator:DescribeAccelerator",
        "globalaccelerator:DescribeCrossAccountAttachment",
        "globalaccelerator:DescribeEndpointGroup",
        "globalaccelerator:DescribeListener",
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListCrossAccountAttachments",
        "globalaccelerator:ListEndpointGroups",
        "globalaccelerator:ListListeners",
        "globalaccelerator:ListTagsForResource",
        "glue:BatchGetDevEndpoints",
        "glue:BatchGetJobs",
        "glue:BatchGetWorkflows",
        "glue:GetClassifier",
        "glue:GetClassifiers",
        "glue:GetCrawler",
        "glue:GetCrawlers",
        "glue:GetDataCatalogEncryptionSettings",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetDevEndpoint",
        "glue:GetDevEndpoints",
        "glue:GetJob",
        "glue:GetJobs",
        "glue:GetMLTransform",
        "glue:GetMLTransforms",
```

```
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetRegistry",
        "glue:GetSecurityConfiguration",
        "glue:GetSecurityConfigurations",
        "glue:GetTable",
        "glue:GetTags",
        "glue:GetTrigger",
        "glue:GetWorkflow",
        "glue:ListCrawlers",
        "glue:ListDevEndpoints",
        "glue:ListJobs",
        "glue:ListMLTransforms",
        "glue:ListRegistries",
        "glue:ListTriggers",
        "glue:ListWorkflows",
        "grafana:DescribeWorkspace",
        "grafana:DescribeWorkspaceAuthentication",
        "grafana:DescribeWorkspaceConfiguration",
        "grafana:ListWorkspaces",
        "greengrass:DescribeComponent",
        "greengrass:GetComponent",
        "greengrass: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:GetMalwareProtectionPlan",
        "guardduty:GetMasterAccount",
        "guardduty:GetMemberDetectors",
        "guardduty:GetMembers",
        "guardduty:GetThreatIntelSet",
        "guardduty:ListDetectors",
        "guardduty:ListFilters",
```

```
        "guardduty:ListFindings",
        "guardduty:ListIPSets",
        "guardduty:ListMalwareProtectionPlans",
        "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:ListPolicies",
        "iam:ListPolicyVersions",
```

```
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListSAMLProviders",
        "iam:ListServerCertificates",
        "iam:ListUserPolicies",
        "iam:ListUsers",
        "iam:ListVirtualMFADevices",
        "identitystore:DescribeGroup",
        "identitystore:DescribeGroupMembership",
        "identitystore:ListGroupMemberships",
        "identitystore:ListGroupMembershipsForMember",
        "identitystore:ListGroups",
        "imagebuilder:GetComponent",
        "imagebuilder:GetContainerRecipe",
        "imagebuilder:GetDistributionConfiguration",
        "imagebuilder:GetImage",
        "imagebuilder:GetImagePipeline",
        "imagebuilder:GetImageRecipe",
        "imagebuilder:GetInfrastructureConfiguration",
        "imagebuilder:GetLifecyclePolicy",
        "imagebuilder:ListComponentBuildVersions",
        "imagebuilder:ListComponents",
        "imagebuilder:ListContainerRecipes",
        "imagebuilder:ListDistributionConfigurations",
        "imagebuilder:ListImageBuildVersions",
        "imagebuilder:ListImagePipelines",
        "imagebuilder:ListImageRecipes",
        "imagebuilder:ListImages",
        "imagebuilder:ListInfrastructureConfigurations",
        "imagebuilder:ListLifecyclePolicies",
        "inspector2:BatchGetAccountStatus",
        "inspector2:GetDelegatedAdminAccount",
        "inspector2:ListFilters",
        "inspector2:ListMembers",
        "internetmonitor:GetMonitor",
        "internetmonitor:ListMonitors",
        "internetmonitor:ListTagsForResource",
        "iot:DescribeAccountAuditConfiguration",
        "iot:DescribeAuthorizer",
        "iot:DescribeBillingGroup",
        "iot:DescribeCACertificate",
        "iot:DescribeCertificate",
        "iot:DescribeCertificateProvider",
        "iot:DescribeCustomMetric",
```

```
        "iot:DescribeDimension",
        "iot:DescribeDomainConfiguration",
        "iot:DescribeFleetMetric",
        "iot:DescribeJobTemplate",
        "iot:DescribeMitigationAction",
        "iot:DescribeProvisioningTemplate",
        "iot:DescribeRoleAlias",
        "iot:DescribeScheduledAudit",
        "iot:DescribeSecurityProfile",
        "iot:DescribeThingGroup",
        "iot:DescribeThingType",
        "iot:GetPackage",
        "iot:GetPackageVersion",
        "iot:GetPolicy",
        "iot:GetTopicRule",
        "iot:GetTopicRuleDestination",
        "iot:ListAuthorizers",
        "iot:ListBillingGroups",
        "iot:ListCACertificates",
        "iot:ListCertificateProviders",
        "iot:ListCertificates",
        "iot:ListCustomMetrics",
        "iot:ListDimensions",
        "iot:ListDomainConfigurations",
        "iot:ListFleetMetrics",
        "iot:ListJobTemplates",
        "iot:ListMitigationActions",
        "iot:ListPackageVersions",
        "iot:ListPackages",
        "iot:ListPolicies",
        "iot:ListProvisioningTemplates",
        "iot:ListRoleAliases",
        "iot:ListScheduledAudits",
        "iot:ListSecurityProfiles",
        "iot:ListSecurityProfilesForTarget",
        "iot:ListTagsForResource",
        "iot:ListTargetsForSecurityProfile",
        "iot:ListThingGroups",
        "iot:ListThingTypes",
        "iot:ListTopicRuleDestinations",
        "iot:ListTopicRules",
        "iot:ListV2LoggingLevels",
        "iot:ValidateSecurityProfileBehaviors",
        "iotanalytics:DescribeChannel",
```

```
        "iotanalytics:DescribeDataset",
        "iotanalytics:DescribeDatastore",
        "iotanalytics:DescribePipeline",
        "iotanalytics:ListChannels",
        "iotanalytics:ListDatasets",
        "iotanalytics:ListDatastores",
        "iotanalytics:ListPipelines",
        "iotanalytics:ListTagsForResource",
        "iotdeviceadvisor:GetSuiteDefinition",
        "iotdeviceadvisor:ListSuiteDefinitions",
        "iotevents:DescribeAlarmModel",
        "iotevents:DescribeDetectorModel",
        "iotevents:DescribeInput",
        "iotevents:ListAlarmModels",
        "iotevents:ListDetectorModels",
        "iotevents:ListInputs",
        "iotevents:ListTagsForResource",
        "iotfleetwise:GetDecoderManifest",
        "iotfleetwise:GetFleet",
        "iotfleetwise:GetModelManifest",
        "iotfleetwise:GetSignalCatalog",
        "iotfleetwise:GetVehicle",
        "iotfleetwise:ListDecoderManifestNetworkInterfaces",
        "iotfleetwise:ListDecoderManifests",
        "iotfleetwise:ListDecoderManifestSignals",
        "iotfleetwise:ListFleets",
        "iotfleetwise:ListModelManifestNodes",
        "iotfleetwise:ListModelManifests",
        "iotfleetwise:ListSignalCatalogNodes",
        "iotfleetwise:ListSignalCatalogs",
        "iotfleetwise:ListTagsForResource",
        "iotfleetwise:ListVehicles",
        "iotsitewise:DescribeAccessPolicy",
        "iotsitewise:DescribeAsset",
        "iotsitewise:DescribeAssetModel",
        "iotsitewise:DescribeDashboard",
        "iotsitewise:DescribeGateway",
        "iotsitewise:DescribePortal",
        "iotsitewise:DescribeProject",
        "iotsitewise:ListAccessPolicies",
        "iotsitewise:ListAssetModelCompositeModels",
        "iotsitewise:ListAssetModelProperties",
        "iotsitewise:ListAssetModels",
        "iotsitewise:ListAssetProperties",
```

```
        "iotsitewise:ListAssets",
        "iotsitewise:ListAssociatedAssets",
        "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:GetDestination",
        "iotwireless:GetDeviceProfile",
        "iotwireless:GetFuotaTask",
        "iotwireless:GetMulticastGroup",
        "iotwireless:GetNetworkAnalyzerConfiguration",
        "iotwireless:GetServiceProfile",
        "iotwireless:GetWirelessDevice",
        "iotwireless:GetWirelessGateway",
        "iotwireless:GetWirelessGatewayTaskDefinition",
        "iotwireless:ListDestinations",
        "iotwireless:ListDeviceProfiles",
        "iotwireless:ListFuotaTasks",
        "iotwireless:ListMulticastGroups",
        "iotwireless:ListNetworkAnalyzerConfigurations",
        "iotwireless:ListServiceProfiles",
        "iotwireless:ListTagsForResource",
        "iotwireless:ListWirelessDevices",
        "iotwireless:ListWirelessGateways",
        "iotwireless:ListWirelessGatewayTaskDefinitions",
        "ivs:GetChannel",
        "ivs:GetEncoderConfiguration",
        "ivs:GetPlaybackKeyPair",
        "ivs:GetPlaybackRestrictionPolicy",
        "ivs:GetRecordingConfiguration",
        "ivs:GetStage",
```

```
        "ivs:GetStorageConfiguration",
        "ivs:GetStreamKey",
        "ivs:ListChannels",
        "ivs:ListEncoderConfigurations",
        "ivs:ListPlaybackKeyPairs",
        "ivs:ListPlaybackRestrictionPolicies",
        "ivs:ListPublicKeys",
        "ivs:ListRecordingConfigurations",
        "ivs:ListStages",
        "ivs:ListStorageConfigurations",
        "ivs:ListStreamKeys",
        "ivs:ListTagsForResource",
        "ivschat:GetLoggingConfiguration",
        "ivschat:GetRoom",
        "ivschat:ListLoggingConfigurations",
        "ivschat:ListRooms",
        "ivschat:ListTagsForResource",
        "kafka:DescribeCluster",
        "kafka:DescribeClusterV2",
        "kafka:DescribeConfiguration",
        "kafka:DescribeConfigurationRevision",
        "kafka:DescribeVpcConnection",
        "kafka:GetClusterPolicy",
        "kafka:ListClusters",
        "kafka:ListClustersV2",
        "kafka:ListConfigurations",
        "kafka:ListScramSecrets",
        "kafka:ListTagsForResource",
        "kafka:ListVpcConnections",
        "kafkaconnect:DescribeConnector",
        "kafkaconnect:DescribeCustomPlugin",
        "kafkaconnect:DescribeWorkerConfiguration",
        "kafkaconnect:ListConnectors",
        "kafkaconnect:ListCustomPlugins",
        "kafkaconnect:ListTagsForResource",
        "kafkaconnect:ListWorkerConfigurations",
        "kendra:DescribeIndex",
        "kendra:ListIndices",
        "kendra:ListTagsForResource",
        "kinesis:DescribeStreamConsumer",
        "kinesis:DescribeStreamSummary",
        "kinesis:GetResourcePolicy",
        "kinesis:ListStreamConsumers",
        "kinesis:ListStreams",
```

```
        "kinesis:ListTagsForStream",
        "kinesisanalytics:DescribeApplication",
        "kinesisanalytics:ListApplications",
        "kinesisanalytics:ListTagsForResource",
        "kinesisvideo:DescribeSignalingChannel",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:ListSignalingChannels",
        "kinesisvideo:ListStreams",
        "kinesisvideo:ListTagsForResource",
        "kinesisvideo:ListTagsForStream",
        "kms:DescribeKey",
        "kms:GetKeyPolicy",
        "kms:GetKeyRotationStatus",
        "kms:ListAliases",
        "kms:ListKeys",
        "kms:ListResourceTags",
        "lakeformation:DescribeLakeFormationIdentityCenterConfiguration",
        "lakeformation:DescribeResource",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:ListDataCellsFilter",
        "lakeformation:ListPermissions",
        "lakeformation:ListResources",
        "lambda:GetAlias",
        "lambda:GetCodeSigningConfig",
        "lambda:GetEventSourceMapping",
        "lambda:GetFunction",
        "lambda:GetFunctionCodeSigningConfig",
        "lambda:GetFunctionConfiguration",
        "lambda:GetFunctionUrlConfig",
        "lambda:GetLayerVersion",
        "lambda:GetPolicy",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:GetRuntimeManagementConfig",
        "lambda:ListAliases",
        "lambda:ListCodeSigningConfigs",
        "lambda:ListEventSourceMappings",
        "lambda:ListFunctionEventInvokeConfigs",
        "lambda:ListFunctionUrlConfigs",
        "lambda:ListFunctions",
        "lambda:ListLayers",
        "lambda:ListLayerVersions",
        "lambda:ListTags",
        "lambda:ListVersionsByFunction",
        "launchwizard:GetDeployment",
```

```
        "launchwizard:ListDeploymentEvents",
        "launchwizard:ListDeployments",
        "launchwizard:ListTagsForResource",
        "lex:DescribeBot",
        "lex:DescribeBotAlias",
        "lex:DescribeBotVersion",
        "lex:DescribeResourcePolicy",
        "lex:ListBotAliases",
        "lex:ListBotLocales",
        "lex:ListBots",
        "lex:ListBotVersions",
        "lex:ListTagsForResource",
        "license-manager:GetGrant",
        "license-manager:GetLicense",
        "license-manager:ListDistributedGrants",
        "license-manager:ListLicenses",
        "license-manager:ListReceivedGrants",
        "lightsail:GetActiveNames",
        "lightsail:GetAlarms",
        "lightsail:GetBuckets",
        "lightsail:GetCertificates",
        "lightsail:GetContainerServices",
        "lightsail:GetDisk",
        "lightsail:GetDisks",
        "lightsail:GetDistributions",
        "lightsail:GetDomain",
        "lightsail:GetDomains",
        "lightsail:GetInstance",
        "lightsail:GetInstanceSnapshot",
        "lightsail:GetInstanceSnapshots",
        "lightsail:GetInstances",
        "lightsail:GetKeyPair",
        "lightsail:GetLoadBalancer",
        "lightsail:GetLoadBalancers",
        "lightsail:GetLoadBalancerTlsCertificates",
        "lightsail:GetOperations",
        "lightsail:GetRelationalDatabase",
        "lightsail:GetRelationalDatabaseParameters",
        "lightsail:GetRelationalDatabases",
        "lightsail:GetStaticIp",
        "lightsail:GetStaticIps",
        "logs:DescribeAccountPolicies",
        "logs:DescribeDeliveries",
        "logs:DescribeDeliveryDestinations",
```

```
        "logs:DescribeDeliverySources",
        "logs:DescribeDestinations",
        "logs:DescribeIndexPolicies",
        "logs:DescribeLogGroups",
        "logs:DescribeMetricFilters",
        "logs:DescribeResourcePolicies",
        "logs:GetDataProtectionPolicy",
        "logs:GetDelivery",
        "logs:GetDeliveryDestination",
        "logs:GetDeliveryDestinationPolicy",
        "logs:GetDeliverySource",
        "logs:GetLogAnomalyDetector",
        "logs:GetLogDelivery",
        "logs:ListLogAnomalyDetectors",
        "logs:ListLogDeliveries",
        "logs:ListTagsForResource",
        "logs:ListTagsLogGroup",
        "lookoutequipment:DescribeInferenceScheduler",
        "lookoutequipment:ListTagsForResource",
        "lookoutmetrics:DescribeAlert",
        "lookoutmetrics:DescribeAnomalyDetector",
        "lookoutmetrics:ListAlerts",
        "lookoutmetrics:ListAnomalyDetectors",
        "lookoutmetrics:ListMetricSets",
        "lookoutmetrics:ListTagsForResource",
        "lookoutvision:DescribeProject",
        "lookoutvision:ListProjects",
        "m2:GetEnvironment",
        "m2:ListEnvironments",
        "m2:ListTagsForResource",
        "macie2:DescribeOrganizationConfiguration",
        "macie2:GetAllowList",
        "macie2:GetAutomatedDiscoveryConfiguration",
        "macie2:GetClassificationExportConfiguration",
        "macie2:GetCustomDataIdentifier",
        "macie2:GetFindingsPublicationConfiguration",
        "macie2:GetMacieSession",
        "macie2:ListAllowLists",
        "macie2:ListAutomatedDiscoveryAccounts",
        "macie2:ListCustomDataIdentifiers",
        "macie2:ListTagsForResource",
        "managedblockchain:GetAccessor",
        "managedblockchain:GetMember",
        "managedblockchain:GetNetwork",
```

```
        "managedblockchain:GetNode",
        "managedblockchain:ListAccessors",
        "managedblockchain:ListInvitations",
        "managedblockchain:ListMembers",
        "managedblockchain:ListNodes",
        "mediaconnect:DescribeBridge",
        "mediaconnect:DescribeFlow",
        "mediaconnect:DescribeGateway",
        "mediaconnect:ListBridges",
        "mediaconnect:ListFlows",
        "mediaconnect:ListGateways",
        "mediaconnect:ListTagsForResource",
        "medialive:DescribeChannelPlacementGroup",
        "medialive:DescribeMultiplexProgram",
        "medialive:ListChannelPlacementGroups",
        "medialive:ListMultiplexPrograms",
        "medialive:ListMultiplexes",
        "medialive:ListTagsForResource",
        "mediapackage-vod:DescribeAsset",
        "mediapackage-vod:DescribePackagingConfiguration",
        "mediapackage-vod:DescribePackagingGroup",
        "mediapackage-vod:ListAssets",
        "mediapackage-vod:ListPackagingConfigurations",
        "mediapackage-vod:ListPackagingGroups",
        "mediapackage-vod:ListTagsForResource",
        "mediapackagev2:GetChannel",
        "mediapackagev2:GetChannelGroup",
        "mediapackagev2:GetOriginEndpoint",
        "mediapackagev2:ListChannelGroups",
        "mediapackagev2:ListChannels",
        "mediapackagev2:ListOriginEndpoints",
        "mediatailor:DescribeChannel",
        "mediatailor:DescribeLiveSource",
        "mediatailor:DescribeSourceLocation",
        "mediatailor:DescribeVodSource",
        "mediatailor:GetPlaybackConfiguration",
        "mediatailor:ListChannels",
        "mediatailor:ListLiveSources",
        "mediatailor:ListPlaybackConfigurations",
        "mediatailor:ListSourceLocations",
        "mediatailor:ListVodSources",
        "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:GetTransitGatewayPeering",
        "networkmanager:GetTransitGatewayRegistrations",
        "networkmanager:ListConnectPeers",
        "networkmanager:ListPeerings",
        "networkmanager:ListTagsForResource",
        "nimble:GetLaunchProfile",
        "nimble:GetLaunchProfileDetails",
        "nimble:GetStreamingImage",
        "nimble:GetStudio",
        "nimble:GetStudioComponent",
        "nimble:ListLaunchProfiles",
        "nimble:ListStreamingImages",
        "nimble:ListStudioComponents",
        "nimble:ListStudios",
        "oam:GetSink",
        "oam:GetSinkPolicy",
```

```
        "oam:ListSinks",
        "omics:GetAnnotationStore",
        "omics:GetRunGroup",
        "omics:GetSequenceStore",
        "omics:GetVariantStore",
        "omics:GetWorkflow",
        "omics:ListAnnotationStores",
        "omics:ListRunGroups",
        "omics:ListSequenceStores",
        "omics:ListTagsForResource",
        "omics:ListVariantStores",
        "omics:ListWorkflows",
        "opsworks:DescribeInstances",
        "opsworks:DescribeLayers",
        "opsworks:DescribeTimeBasedAutoScaling",
        "opsworks:DescribeVolumes",
        "opsworks:ListTags",
        "organizations:DescribeAccount",
        "organizations:DescribeEffectivePolicy",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribePolicy",
        "organizations:DescribeResourcePolicy",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
        "organizations:ListRoots",
        "organizations:ListTagsForResource",
        "organizations:ListTargetsForPolicy",
        "osis:GetPipeline",
        "osis:ListPipelines",
        "osis:ListTagsForResource",
        "panorama:DescribeApplicationInstance",
        "panorama:DescribeApplicationInstanceDetails",
        "panorama:DescribePackage",
        "panorama:DescribePackageVersion",
        "panorama:ListApplicationInstances",
        "panorama:ListNodes",
        "panorama:ListPackages",
        "payment-cryptography:GetAlias",
```

```
        "payment-cryptography:GetKey",
        "payment-cryptography:ListAliases",
        "payment-cryptography:ListKeys",
        "payment-cryptography:ListTagsForResource",
        "pca-connector-ad:GetConnector",
        "pca-connector-ad:GetDirectoryRegistration",
        "pca-connector-ad:ListConnectors",
        "pca-connector-ad:ListDirectoryRegistrations",
        "pca-connector-ad:ListTagsForResource",
        "pca-connector-scep:GetConnector",
        "pca-connector-scep:ListConnectors",
        "pca-connector-scep:ListTagsForResource",
        "personalize:DescribeDataset",
        "personalize:DescribeDatasetGroup",
        "personalize:DescribeSchema",
        "personalize:DescribeSolution",
        "personalize:ListDatasetGroups",
        "personalize:ListDatasetImportJobs",
        "personalize:ListDatasets",
        "personalize:ListSchemas",
        "personalize:ListSolutions",
        "personalize:ListTagsForResource",
        "pipes:DescribePipe",
        "pipes:ListPipes",
        "profile:GetDomain",
        "profile:GetIntegration",
        "profile:GetProfileObjectType",
        "profile:ListDomains",
        "profile:ListIntegrations",
        "profile:ListProfileObjectTypes",
        "profile:ListTagsForResource",
        "qbusiness:GetApplication",
        "qbusiness:ListApplications",
        "qbusiness:ListTagsForResource",
        "quicksight:DescribeAccountSubscription",
        "quicksight:DescribeAnalysis",
        "quicksight:DescribeAnalysisPermissions",
        "quicksight:DescribeDashboard",
        "quicksight:DescribeDashboardPermissions",
        "quicksight:DescribeDataSet",
        "quicksight:DescribeDataSetPermissions",
        "quicksight:DescribeDataSetRefreshProperties",
        "quicksight:DescribeDataSource",
        "quicksight:DescribeDataSourcePermissions",
```

```
        "quicksight:DescribeRefreshSchedule",
        "quicksight:DescribeTemplate",
        "quicksight:DescribeTemplatePermissions",
        "quicksight:DescribeTheme",
        "quicksight:DescribeThemePermissions",
        "quicksight:DescribeTopic",
        "quicksight:ListAnalyses",
        "quicksight:ListDashboards",
        "quicksight:ListDataSets",
        "quicksight:ListDataSources",
        "quicksight:ListRefreshSchedules",
        "quicksight:ListTagsForResource",
        "quicksight:ListTemplates",
        "quicksight:ListThemes",
        "quicksight:ListTopics",
        "ram:GetPermission",
        "ram:GetResourceShareAssociations",
        "ram:GetResourceShares",
        "ram:ListPermissionAssociations",
        "ram:ListPermissions",
        "ram:ListPermissionVersions",
        "ram:ListResources",
        "ram:ListResourceSharePermissions",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBProxies",
        "rds:DescribeDBProxyEndpoints",
        "rds:DescribeDBProxyTargetGroups",
        "rds:DescribeDBProxyTargets",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBShardGroups",
        "rds:DescribeDBSnapshotAttributes",
        "rds:DescribeDBSnapshots",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultClusterParameters",
        "rds:DescribeEngineDefaultParameters",
        "rds:DescribeEventSubscriptions",
```

```
        "rds:DescribeGlobalClusters",
        "rds:DescribeIntegrations",
        "rds:DescribeOptionGroups",
        "rds:ListTagsForResource",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListSnapshotCopyConfigurations",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:ListWorkgroups",
        "redshift:DescribeClusterParameterGroups",
        "redshift:DescribeClusterParameters",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSecurityGroups",
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeClusterSubnetGroups",
        "redshift:DescribeEndpointAccess",
        "redshift:DescribeEndpointAuthorization",
        "redshift:DescribeEventSubscriptions",
        "redshift:DescribeIntegrations",
        "redshift:DescribeLoggingStatus",
        "redshift:DescribeScheduledActions",
        "redshift:DescribeTags",
        "redshift:GetResourcePolicy",
        "refactor-spaces:GetEnvironment",
        "refactor-spaces:GetService",
        "refactor-spaces:ListApplications",
        "refactor-spaces:ListEnvironments",
        "refactor-spaces:ListServices",
        "refactor-spaces:ListTagsForResource",
        "rekognition:DescribeProjects",
        "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",
        "rolesanywhere:GetCrl",
        "rolesanywhere:GetProfile",
        "rolesanywhere:GetTrustAnchor",
        "rolesanywhere:ListCrls",
        "rolesanywhere:ListProfiles",
        "rolesanywhere:ListTagsForResource",
        "rolesanywhere:ListTrustAnchors",
        "route53-recovery-control-config:DescribeCluster",
        "route53-recovery-control-config:DescribeControlPanel",
        "route53-recovery-control-config:DescribeRoutingControl",
        "route53-recovery-control-config:DescribeSafetyRule",
        "route53-recovery-control-config:ListClusters",
        "route53-recovery-control-config:ListControlPanels",
        "route53-recovery-control-config:ListRoutingControls",
        "route53-recovery-control-config:ListSafetyRules",
        "route53-recovery-control-config:ListTagsForResource",
        "route53-recovery-readiness:GetCell",
        "route53-recovery-readiness:GetReadinessCheck",
        "route53-recovery-readiness:GetRecoveryGroup",
        "route53-recovery-readiness:GetResourceSet",
        "route53-recovery-readiness:ListCells",
        "route53-recovery-readiness:ListReadinessChecks",
        "route53-recovery-readiness:ListRecoveryGroups",
        "route53-recovery-readiness:ListResourceSets",
        "route53:GetChange",
        "route53:GetDNSSEC",
        "route53:GetHealthCheck",
        "route53:GetHostedZone",
        "route53:ListCidrBlocks",
        "route53:ListCidrCollections",
        "route53:ListCidrLocations",
        "route53:ListHealthChecks",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName",
```

```
            "route53:ListQueryLoggingConfigs",
            "route53:ListResourceRecordSets",
            "route53:ListTagsForResource",
            "route53profiles:GetProfile",
            "route53profiles:GetProfileAssociation",
            "route53profiles:ListProfileAssociations",
            "route53profiles:ListProfiles",
            "route53profiles:ListTagsForResource",
            "route53resolver:GetFirewallDomainList",
            "route53resolver:GetFirewallRuleGroup",
            "route53resolver:GetFirewallRuleGroupAssociation",
            "route53resolver: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:GetAccessGrant",
        "s3:GetAccessGrantsInstance",
        "s3:GetAccessGrantsLocation",
        "s3:GetAccessPoint",
        "s3:GetAccessPointForObjectLambda",
        "s3:GetAccessPointPolicy",
        "s3:GetAccessPointPolicyForObjectLambda",
        "s3:GetAccessPointPolicyStatus",
        "s3:GetAccessPointPolicyStatusForObjectLambda",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetBucketAbac",
        "s3:GetBucketAcl",
        "s3:GetBucketCORS",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketNotification",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketRequestPayment",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "s3:GetBucketWebsite",
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetMultiRegionAccessPoint",
        "s3:GetMultiRegionAccessPointPolicy",
        "s3:GetMultiRegionAccessPointPolicyStatus",
        "s3:GetReplicationConfiguration",
        "s3:GetStorageLensConfiguration",
        "s3:GetStorageLensConfigurationTagging",
        "s3:GetStorageLensGroup",
        "s3:ListAccessGrants",
        "s3:ListAccessGrantsInstances",
        "s3:ListAccessGrantsLocations",
        "s3:ListAccessPoints",
        "s3:ListAccessPointsForObjectLambda",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListMultiRegionAccessPoints",
        "s3:ListStorageLensConfigurations",
        "s3:ListStorageLensGroups",
        "s3:ListTagsForResource",
```

```
        "s3express:GetBucketPolicy",
        "s3express:GetEncryptionConfiguration",
        "s3express:GetLifecycleConfiguration",
        "s3express:ListAllMyDirectoryBuckets",
        "s3tables:GetTableBucket",
        "s3tables:GetTableBucketEncryption",
        "s3tables:GetTableBucketMaintenanceConfiguration",
        "s3tables:GetTableBucketPolicy",
        "s3tables:ListTableBuckets",
        "sagemaker:DescribeApp",
        "sagemaker:DescribeAppImageConfig",
        "sagemaker:DescribeCluster",
        "sagemaker:DescribeCodeRepository",
        "sagemaker:DescribeDataQualityJobDefinition",
        "sagemaker:DescribeDeviceFleet",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeFeatureGroup",
        "sagemaker:DescribeImage",
        "sagemaker:DescribeImageVersion",
        "sagemaker:DescribeInferenceComponent",
        "sagemaker:DescribeInferenceExperiment",
        "sagemaker:DescribeMlflowTrackingServer",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeModelBiasJobDefinition",
        "sagemaker:DescribeModelCard",
        "sagemaker:DescribeModelExplainabilityJobDefinition",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribeModelQualityJobDefinition",
        "sagemaker:DescribeMonitoringSchedule",
        "sagemaker:DescribeNotebookInstance",
        "sagemaker:DescribeNotebookInstanceLifecycleConfig",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeProject",
        "sagemaker:DescribeStudioLifecycleConfig",
        "sagemaker:DescribeUserProfile",
        "sagemaker:DescribeWorkteam",
        "sagemaker:GetModelPackageGroupPolicy",
        "sagemaker:ListAppImageConfigs",
        "sagemaker:ListApps",
        "sagemaker:ListClusters",
```

```
        "sagemaker:ListCodeRepositories",
        "sagemaker:ListDataQualityJobDefinitions",
        "sagemaker:ListDeviceFleets",
        "sagemaker:ListDomains",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListEndpoints",
        "sagemaker:ListFeatureGroups",
        "sagemaker:ListImages",
        "sagemaker:ListImageVersions",
        "sagemaker:ListInferenceComponents",
        "sagemaker:ListInferenceExperiments",
        "sagemaker:ListMlflowTrackingServers",
        "sagemaker:ListModelBiasJobDefinitions",
        "sagemaker:ListModelCardVersions",
        "sagemaker:ListModelCards",
        "sagemaker:ListModelExplainabilityJobDefinitions",
        "sagemaker:ListModelPackageGroups",
        "sagemaker:ListModelPackages",
        "sagemaker:ListModelQualityJobDefinitions",
        "sagemaker:ListModels",
        "sagemaker:ListMonitoringSchedules",
        "sagemaker:ListNotebookInstanceLifecycleConfigs",
        "sagemaker:ListNotebookInstances",
        "sagemaker:ListPipelines",
        "sagemaker:ListProcessingJobs",
        "sagemaker:ListProjects",
        "sagemaker:ListStudioLifecycleConfigs",
        "sagemaker:ListTags",
        "sagemaker:ListUserProfiles",
        "sagemaker:ListWorkteams",
        "scheduler:GetSchedule",
        "scheduler:GetScheduleGroup",
        "scheduler:ListScheduleGroups",
        "scheduler:ListSchedules",
        "scheduler:ListTagsForResource",
        "schemas:DescribeDiscoverer",
        "schemas:DescribeRegistry",
        "schemas:DescribeSchema",
        "schemas:GetResourcePolicy",
        "schemas:ListDiscoverers",
        "schemas:ListRegistries",
        "schemas:ListSchemas",
        "sdb:GetAttributes",
        "sdb:ListDomains",
```

```
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:ListSecrets",
        "secretsmanager:ListSecretVersionIds",
        "securityhub:DescribeHub",
        "securityhub:DescribeStandardsControls",
        "securityhub:GetEnabledStandards",
        "securitylake:GetSubscriber",
        "securitylake:ListDataLakeExceptions",
        "securitylake:ListDataLakes",
        "securitylake:ListLogSources",
        "securitylake:ListSubscribers",
        "securitylake:ListTagsForResource",
        "serviceCatalog:DescribePortfolioShares",
        "servicecatalog:DescribeServiceAction",
        "servicecatalog:GetAttributeGroup",
        "servicecatalog:ListApplications",
        "servicecatalog:ListAssociatedResources",
        "servicecatalog:ListAttributeGroups",
        "servicecatalog:ListServiceActions",
        "servicecatalog:ListServiceActionsForProvisioningArtifact",
        "servicediscovery:GetInstance",
        "servicediscovery:GetNamespace",
        "servicediscovery:GetService",
        "servicediscovery:ListInstances",
        "servicediscovery:ListNamespaces",
        "servicediscovery:ListServices",
        "servicediscovery:ListTagsForResource",
        "ses:DescribeReceiptRule",
        "ses:DescribeReceiptRuleSet",
        "ses:GetConfigurationSet",
        "ses:GetConfigurationSetEventDestinations",
        "ses:GetContactList",
        "ses:GetDedicatedIpPool",
        "ses:GetDedicatedIps",
        "ses:GetEmailTemplate",
        "ses:GetTemplate",
        "ses:GetTrafficPolicy",
        "ses:ListConfigurationSets",
        "ses:ListContactLists",
        "ses:ListDedicatedIpPools",
        "ses:ListEmailTemplates",
        "ses:ListReceiptFilters",
        "ses:ListReceiptRuleSets",
```

```
        "ses:ListTagsForResource",
        "ses:ListTemplates",
        "ses:ListTrafficPolicies",
        "shield:DescribeDRTAccess",
        "shield:DescribeProtection",
        "shield:DescribeProtectionGroup",
        "shield:DescribeSubscription",
        "shield:ListProtectionGroups",
        "shield:ListTagsForResource",
        "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-contacts:GetContact",
        "ssm-contacts:GetContactChannel",
        "ssm-contacts:ListContactChannels",
        "ssm-contacts:ListContacts",
        "ssm-contacts:ListTagsForResource",
        "ssm-incidents:GetReplicationSet",
        "ssm-incidents:GetResponsePlan",
        "ssm-incidents:ListReplicationSets",
        "ssm-incidents:ListResponsePlans",
        "ssm-incidents:ListTagsForResource",
        "ssm-quicksetup:GetConfigurationManager",
        "ssm-quicksetup:ListConfigurationManagers",
        "ssm-sap:ListTagsForResource",
        "ssm:DescribeAssociation",
        "ssm:DescribeAutomationExecutions",
        "ssm:DescribeDocument",
        "ssm:DescribeDocumentPermission",
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeMaintenanceWindows",
        "ssm:DescribeParameters",
        "ssm:DescribePatchBaselines",
```

```
        "ssm:GetAutomationExecution",
        "ssm:GetDefaultPatchBaseline",
        "ssm:GetDocument",
        "ssm:GetPatchBaseline",
        "ssm:GetResourcePolicies",
        "ssm:GetServiceSetting",
        "ssm:ListAssociations",
        "ssm:ListDocuments",
        "ssm:ListResourceDataSync",
        "ssm:ListTagsForResource",
        "sso:DescribeInstanceAccessControlAttributeConfiguration",
        "sso:DescribePermissionSet",
        "sso:GetInlinePolicyForPermissionSet",
        "sso:ListManagedPoliciesInPermissionSet",
        "sso:ListPermissionSets",
        "sso:ListTagsForResource",
        "states:DescribeActivity",
        "states:DescribeStateMachine",
        "states:DescribeStateMachineAlias",
        "states:ListActivities",
        "states:ListStateMachineAliases",
        "states:ListStateMachines",
        "states:ListTagsForResource",
        "storagegateway:ListGateways",
        "storagegateway:ListTagsForResource",
        "storagegateway:ListVolumes",
        "sts:GetCallerIdentity",
        "support:DescribeCases",
        "synthetics:DescribeCanaries",
        "synthetics:DescribeCanariesLastRun",
        "synthetics:DescribeRuntimeVersions",
        "synthetics:GetCanary",
        "synthetics:GetCanaryRuns",
        "synthetics:GetGroup",
        "synthetics:ListAssociatedGroups",
        "synthetics:ListGroupResources",
        "synthetics:ListGroups",
        "synthetics:ListTagsForResource",
        "tag:GetResources",
        "timestream:DescribeDatabase",
        "timestream:DescribeEndpoints",
        "timestream:DescribeTable",
        "timestream:ListDatabases",
        "timestream:ListTables",
```

```
        "timestream:ListTagsForResource",
        "transfer:DescribeAgreement",
        "transfer:DescribeCertificate",
        "transfer:DescribeConnector",
        "transfer:DescribeProfile",
        "transfer:DescribeServer",
        "transfer:DescribeUser",
        "transfer:DescribeWorkflow",
        "transfer:ListAgreements",
        "transfer:ListCertificates",
        "transfer:ListConnectors",
        "transfer:ListProfiles",
        "transfer:ListServers",
        "transfer:ListTagsForResource",
        "transfer:ListUsers",
        "transfer:ListWorkflows",
        "verifiedpermissions:GetPolicyStore",
        "verifiedpermissions:GetPolicyTemplate",
        "verifiedpermissions:GetSchema",
        "verifiedpermissions:ListPolicyStores",
        "verifiedpermissions:ListPolicyTemplates",
        "verifiedpermissions:ListTagsForResource",
        "voiceid:DescribeDomain",
        "voiceid:ListTagsForResource",
        "vpc-lattice:GetAccessLogSubscription",
        "vpc-lattice:GetService",
        "vpc-lattice:GetServiceNetwork",
        "vpc-lattice:GetTargetGroup",
        "vpc-lattice:ListAccessLogSubscriptions",
        "vpc-lattice:ListServiceNetworks",
        "vpc-lattice:ListServices",
        "vpc-lattice:ListTagsForResource",
        "vpc-lattice:ListTargetGroups",
        "vpc-lattice:ListTargets",
        "waf-regional:GetLoggingConfiguration",
        "waf-regional:GetWebACL",
        "waf-regional:GetWebACLForResource",
        "waf-regional:ListLoggingConfigurations",
        "waf:GetLoggingConfiguration",
        "waf:GetWebACL",
        "wafv2:GetLoggingConfiguration",
        "wafv2:GetRuleGroup",
        "wafv2:ListLoggingConfigurations",
        "wafv2:ListRuleGroups",
```

```
        "wafv2:ListTagsForResource",
        "workspaces:DescribeConnectionAliases",
        "workspaces:DescribeTags",
        "workspaces:DescribeWorkspaces",
        "xray:GetGroup",
        "xray:GetGroups",
        "xray:GetSamplingRules",
        "xray:ListResourcePolicies",
        "xray:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConfigLogStreamStatementID",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/config/*"
    },
    {
      "Sid" : "ConfigLogEventsStatementID",
      "Effect" : "Allow",
      "Action" : "logs:PutLogEvents",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/config/*:log-stream:config-rule-
evaluation/*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSAccountActivityAccess

説明: アカウントアクティビティページへのアクセスをユーザーに許可します。

AWSAccountActivityAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSAccountActivityAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2023 年 3 月 7 日 17:02 UTC
- ARN: arn:aws:iam::aws:policy/AWSAccountActivityAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSAccountManagementFullAccess

説明: AWS アカウント管理へのフルアクセスを提供します。

`AWSAccountManagementFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSAccountManagementFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 9 月 30 日 23:20 UTC
- 編集日時: 2021 年 9 月 30 日 23:20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountManagementFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSAccountManagementReadOnlyAccess

説明: AWS アカウント管理への読み取り専用アクセスを提供します

`AWSAccountManagementReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSAccountManagementReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2021 年 9 月 30 日 23:29 UTC
- 編集日時: 2021 年 9 月 30 日 23:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountManagementReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSAccountSettingsManagementRole

説明: AWS アプリケーションのアカウントを管理するために必要なアクセス許可を提供します。

AWSAccountSettingsManagementRole は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSAccountSettingsManagementRole をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 12 月 11 日 17:49 UTC
- 編集日時: 2025 年 12 月 11 日 17:49 UTC
- ARN: arn:aws:iam::aws:policy/AWSAccountSettingsManagementRole

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "account:GetContactInformation",
        "account:PutContactInformation",
        "account:GetAccountInformation",
        "account:CloseAccount"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "payments:ListTagsForResource",
        "payments:UntagResource",
        "payments:TagResource",
        "payments:ListPaymentPreferences",
        "payments:GetPaymentInstrument",
        "payments:GetPaymentStatus",
        "payments:MakePayment",
        "payments:UpdatePaymentPreferences",
        "payments:CreatePaymentInstrument",
        "payments:UpdatePaymentInstrument"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "invoicing:GetInvoicePDF"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "billing:GetSellerOfRecord"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "freetier:GetAccountPlanState"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ce:GetCostAndUsage"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "pricing:GetProducts"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "tax:GetTaxRegistration",
        "tax:PutTaxRegistration",
        "tax:ListTaxRegistrations",
        "tax:DeleteTaxRegistration",
        "tax:BatchPutTaxRegistration",
        "tax:GetTaxRegistrationDocument"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "customer-verification:GetCustomerVerificationDetails",
        "customer-verification:GetCustomerVerificationEligibility",
        "customer-verification:CreateCustomerVerificationDetails",
        "customer-verification:CreateUploadUrls",
        "customer-verification:UpdateCustomerVerificationDetails"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sso:ListInstances",
        "sso:ListApplications"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSAccountUsageReportAccess

説明: ユーザーにアカウント使用状況レポートページへのアクセスを許可します。

AWSAccountUsageReportAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSAccountUsageReportAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2015 年 2 月 6 日 18:41 UTC
- ARN: arn:aws:iam::aws:policy/AWSAccountUsageReportAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-portal:ViewUsage"
      ],
```

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSAgentlessDiscoveryService

説明: Discovery Agentless Connector が AWS Application Discovery Service に登録するためのアクセスを提供します。

`AWSAgentlessDiscoveryService` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSAgentlessDiscoveryService` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2016 年 8 月 2 日 01:35 UTC
- 編集日時: 2020 年 2 月 24 日 23:08 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAgentlessDiscoveryService`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSAppFabricFullAccess

説明: AWS AppFabric サービスへのフルアクセスと、S3、Kinesis、KMS などの依存サービスへの読み取り専用アクセスを提供します。

AWSAppFabricFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSAppFabricFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 6 月 27 日 19:51 UTC
- 編集日時: 2023 年 6 月 27 日 19:51 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppFabricFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSAppFabricReadOnlyAccess

説明: AWS AppFabric への読み取り専用アクセスを提供します

AWSAppFabricReadOnlyAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSAppFabricReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 6 月 27 日 19:52 UTC
- 編集日時: 2023 年 6 月 27 日 19:52 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppFabricReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSAppFabricServiceRolePolicy

説明: AppFabric にユーザーに代わって AWS リソースへのアクセスを提供します

AWSAppFabricServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー

- 作成日時: 2023 年 6 月 26 日 21:07 UTC
- 編集日時: 2023 年 6 月 26 日 21:07 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSAppFabricServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSApplicationAutoscalingAppStreamFleetPolicy

説明: AppStream と CloudWatch にアクセスするための許可をアプリケーションの自動スケーリングに付与するポリシーです。

AWSApplicationAutoscalingAppStreamFleetPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー

- 作成日時: 2017 年 10 月 20 日 19:04 UTC
- 編集日時: 2017 年 10 月 20 日 19:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingAppStreamFleetPolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appstream:UpdateFleet",
        "appstream:DescribeFleets",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSApplicationAutoscalingCassandraTablePolicy

説明: Cassandra と CloudWatch にアクセスするための許可をアプリケーションの自動スケーリングに付与するポリシーです。

AWSApplicationAutoscalingCassandraTablePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 3 月 18 日 22:49 UTC
- 編集日時: 2020 年 3 月 18 日 22:49 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingCassandraTablePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSApplicationAutoscalingComprehendEndpointPolicy

説明: Comprehend と CloudWatch にアクセスするための許可をアプリケーションの自動スケーリングに付与するポリシーです。

`AWSApplicationAutoscalingComprehendEndpointPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー

- 作成日時: 2019 年 11 月 14 日 18:39 UTC
- 編集日時: 2019 年 11 月 14 日 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingComprehendEndpointPolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "comprehend:UpdateEndpoint",
        "comprehend:DescribeEndpoint",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSApplicationAutoScalingCustomResourcePolicy

説明: APIGateway と CloudWatch にアクセスしてカスタムリソーススケーリングを行うためのアクセス許可をアプリケーションの自動スケーリングに付与するポリシー

AWSApplicationAutoScalingCustomResourcePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 6 月 4 日 23:22 UTC
- 編集日時: 2018 年 6 月 4 日 23:22 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoScalingCustomResourcePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
        "execute-api:Invoke",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSApplicationAutoscalingDynamoDBTablePolicy

説明: DynamoDB と CloudWatch にアクセスするためのアクセス許可をアプリケーションの自動スケーリングに付与するポリシーです。

`AWSApplicationAutoscalingDynamoDBTablePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 10 月 20 日 21:34 UTC
- 編集日時: 2017 年 10 月 20 日 21:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingDynamoDBTablePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeTable",
        "dynamodb:UpdateTable",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSApplicationAutoscalingEC2SpotFleetRequestPolicy

説明: EC2 スポットフリートと CloudWatch にアクセスするための許可をアプリケーションの自動スケーリングに付与するポリシーです。

AWSApplicationAutoscalingEC2SpotFleetRequestPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 10 月 25 日 18:23 UTC
- 編集日時: 2017 年 10 月 25 日 18:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingEC2SpotFleetRequestPolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSpotFleetRequests",
        "ec2:ModifySpotFleetRequest",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
```

```
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSApplicationAutoscalingECSServicePolicy

説明: EC2 コンテナサービスと CloudWatch にアクセスするための許可をアプリケーションの自動スケーリングに付与するポリシーです。

AWSApplicationAutoscalingECSServicePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 10 月 25 日 23:53 UTC
- 編集日時: 2024 年 10 月 24 日 20:05 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingECSServicePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeServices",
        "ecs:UpdateService",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSApplicationAutoscalingElastiCacheRGPolicy

説明: Amazon ElastiCache と Amazon CloudWatch にアクセスするための許可をアプリケーションの自動スケーリングに付与するポリシーです。

AWSApplicationAutoscalingElastiCacheRGPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 8 月 17 日 23:41 UTC
- 編集日時: 2025 年 3 月 26 日 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingElastiCacheRGPolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ElastiCacheActionsOnAllClusters",
      "Effect" : "Allow",
      "Action" : [
        "elasticache:DescribeReplicationGroups",
        "elasticache:ModifyCacheCluster",
        "elasticache:ModifyReplicationGroupShardConfiguration",
        "elasticache:IncreaseReplicaCount",
        "elasticache:DecreaseReplicaCount",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeCacheParameters"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CloudWatchActionsOnAllAlarms",
      "Effect" : "Allow",
```

```
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:*"
      ]
    },
    {
      "Sid" : "CloudWatchActionsOnTargetTrackingAlarms",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:TargetTracking*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSApplicationAutoscalingEMRInstanceGroupPolicy

説明: Elastic Map Reduce と CloudWatch にアクセスするための許可をアプリケーションの自動スケーリングに付与するポリシーです。

`AWSApplicationAutoscalingEMRInstanceGroupPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 10 月 26 日 00:57 UTC
- 編集日時: 2017 年 10 月 26 日 00:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingEMRInstanceGroupPolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ModifyInstanceGroups",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSApplicationAutoscalingKafkaClusterPolicy

説明: Apache Kafka と CloudWatch のマネージドストリーミングにアクセスするための許可をアプリケーションの自動スケーリングに付与するポリシーです。

AWSApplicationAutoscalingKafkaClusterPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 8 月 24 日 18:36 UTC
- 編集日時: 2020 年 8 月 24 日 18:36 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingKafkaClusterPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
        "kafka:DescribeClusterOperation",
        "kafka:UpdateBrokerStorage",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSApplicationAutoscalingLambdaConcurrencyPolicy

説明: Lambda と CloudWatch にアクセスするための許可をアプリケーションの自動スケーリングに付与するポリシーです。

`AWSApplicationAutoscalingLambdaConcurrencyPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 10 月 21 日 20:04 UTC
- 編集日時: 2019 年 10 月 21 日 20:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingLambdaConcurrencyPolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:PutProvisionedConcurrencyConfig",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:DeleteProvisionedConcurrencyConfig",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSApplicationAutoscalingNeptuneClusterPolicy

説明: Amazon Neptune と Amazon CloudWatch にアクセスするための許可をアプリケーションの自動スケーリングに付与するポリシーです。

AWSApplicationAutoscalingNeptuneClusterPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 9 月 2 日 21:14 UTC
- 編集日時: 2021 年 9 月 2 日 21:14 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingNeptuneClusterPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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*"
```

```
      ]
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSApplicationAutoscalingRDSClusterPolicy

説明: RDS と CloudWatch にアクセスするための許可をアプリケーションの自動スケーリングに付与するポリシーです。

AWSApplicationAutoscalingRDSClusterPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 10 月 17 日 17:46 UTC
- 編集日時: 2018 年 8 月 7 日 19:14 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingRDSClusterPolicy`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSApplicationAutoscalingSageMakerEndpointPolicy

説明: SageMaker と CloudWatch にアクセスするための許可をアプリケーションの自動スケーリングに付与するポリシーです。

AWSApplicationAutoscalingSageMakerEndpointPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 2 月 6 日 19:58 UTC
- 編集日時: 2023 年 11 月 13 日 18:52 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingSageMakerEndpointPolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSApplicationAutoscalingWorkSpacesPoolPolicy

説明: Amazon WorkSpaces と Amazon CloudWatch にアクセスするための許可を Application の自動スケーリング に付与するポリシー。

AWSApplicationAutoscalingWorkSpacesPoolPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2024 年 6 月 17 日 18:39 UTC
- 編集日時: 2024 年 6 月 17 日 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingWorkSpacesPoolPolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "WorkSpacesActionsOnAllPools",
      "Effect" : "Allow",
      "Action" : [
        "workspaces:DescribeWorkspacesPools",
        "workspaces:UpdateWorkspacesPool"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CloudWatchActionsOnAllAlarms",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CloudWatchActionsOnTargetTrackingAlarms",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:TargetTracking*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSApplicationDiscoveryAgentAccess

説明: Discovery Agent が AWS Application Discovery Service に登録するためのアクセスを提供します。

AWSApplicationDiscoveryAgentAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSApplicationDiscoveryAgentAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2016 年 5 月 11 日 21:38 UTC
- 編集日時: 2020 年 2 月 24 日 22:26 UTC
- ARN: arn:aws:iam::aws:policy/AWSApplicationDiscoveryAgentAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:GetHomeRegion"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSApplicationDiscoveryAgentlessCollectorAccess

説明: Application Discovery Service エージェントレスコレクターによる自動更新、登録、および Application Discovery Service との通信を可能にします

`AWSApplicationDiscoveryAgentlessCollectorAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSApplicationDiscoveryAgentlessCollectorAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 8 月 16 日 21:00 UTC
- 編集日時: 2022 年 8 月 16 日 21:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationDiscoveryAgentlessCollectorAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント


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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSApplicationDiscoveryServiceFullAccess

説明: AWS Application Discovery Service によって管理される設定項目を表示およびタグ付けするためのフルアクセスを提供します

AWSApplicationDiscoveryServiceFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSApplicationDiscoveryServiceFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2016 年 5 月 11 日 21:30 UTC
- 編集日時: 2019 年 6 月 19 日 21:21 UTC
- ARN: arn:aws:iam::aws:policy/AWSApplicationDiscoveryServiceFullAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSApplicationMigrationAgentInstallationPolicy

説明: このポリシーでは、 AWS アプリケーション移行サービス (MGN) で外部サーバーを移行するために使用する AWS レプリケーションエージェントをインストールできます AWS。このポリシーを AWS 、レプリケーションエージェントのインストール時に指定した認証情報を持つ IAM ユーザーまたはロールにアタッチします。

`AWSApplicationMigrationAgentInstallationPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSApplicationMigrationAgentInstallationPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 6 月 19 日 07:51 UTC
- 編集日時: 2022 年 9 月 20 日 11:21 UTC
- ARN: arn:aws:iam::aws:policy/AWSApplicationMigrationAgentInstallationPolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSApplicationMigrationAgentPolicy

説明: このポリシーでは、 AWS アプリケーション移行サービス (MGN) で外部サーバーを移行するために使用する AWS レプリケーションエージェントをインストールして使用できます AWS。このポリシーを AWS 、レプリケーションエージェントのインストール時に指定した認証情報を持つ IAM ユーザーまたはロールにアタッチします。

AWSApplicationMigrationAgentPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSApplicationMigrationAgentPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 4 月 7 日 07:00 UTC
- 編集日時: 2022 年 9 月 20 日 11:13 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationAgentPolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSApplicationMigrationAgentPolicy_v2

説明: このポリシーでは、 AWS アプリケーション移行サービス (MGN) で外部サーバーを移行するために使用する AWS レプリケーションエージェントの使用を許可します AWS。IAM ユーザーまたはロールにこのポリシーをアタッチすることはおすすめしません。

AWSApplicationMigrationAgentPolicy_v2 は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSApplicationMigrationAgentPolicy_v2 をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 6 月 6 日 14:14 UTC

- 編集日時: 2022 年 6 月 6 日 14:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationAgentPolicy_v2`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する

- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSApplicationMigrationConversionServerPolicy

説明: このポリシーにより、アプリケーション移行サービスによって起動される EC2 インスタンスであるアプリケーション移行サービス (MGN) 変換サーバーが、MGN サービスと通信できるようになります。このポリシーの付いた IAM ロールは MGN によって (EC2 インスタンスプロファイルとして) MGN 変換サーバーにアタッチされ、MGN は必要に応じて自動的に起動および終了します。IAM ユーザーまたはロールにこのポリシーをアタッチすることはおすすめしません。MGN 変換サーバーは、ユーザーが MGN コンソール、CLI、または API を使用してテストインスタンスまたはカットオーバーインスタンスを起動することを選択したときに、アプリケーション移行サービスによって使用されます。

AWSApplicationMigrationConversionServerPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSApplicationMigrationConversionServerPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2021 年 4 月 7 日 06:48 UTC
- 編集日時: 2021 年 4 月 7 日 06:48 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationConversionServerPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:SendClientMetricsForMgn",
        "mgn:SendClientLogsForMgn",
        "mgn:GetChannelCommandsForMgn",
        "mgn:SendChannelCommandResultForMgn"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSApplicationMigrationEC2Access

説明: このポリシーは、アプリケーション移行サービス (MGN) を使用して移行したサーバーを EC2 インスタンスとして起動するために必要な Amazon EC2 オペレーションを提供します。このポリシーを IAM ユーザーまたはロールにアタッチします。

AWSApplicationMigrationEC2Access は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSApplicationMigrationEC2Access をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 4 月 7 日 07:05 UTC
- 編集日時: 2025 年 2 月 11 日 13:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationEC2Access`

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AWSApplicationMigrationConversionServerRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
```

```
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSnapshots",
        "ec2:DescribeImages",
        "ec2:DescribeVolumes"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
```

```
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteLaunchTemplate"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:GetConsoleOutput",
        "ec2:GetConsoleScreenshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
```

```
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateSecurityGroup",
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateSecurityGroup",
            "CreateVolume",
            "CreateSnapshot",
            "RunInstances",
            "CreateLaunchTemplate"
          ]
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:ModifyVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSApplicationMigrationFullAccess

説明: このポリシーは、 AWS Application Migration Service (MGN) のすべてのパブリック APIs へのアクセス許可と、KMS キー情報を読み取るアクセス許可を提供します。このポリシーを IAM ユーザーまたはロールにアタッチします。

`AWSApplicationMigrationFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSApplicationMigrationFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 4 月 7 日 06:56 UTC
- 編集日時: 2025 年 7 月 2 日 15:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v9 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : [
        "mgn:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor1",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor2",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:DescribeKeyPairs",
        "ec2:DescribeTags",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetEbsDefaultKmsKeyId"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor3",
      "Effect" : "Allow",
      "Action" : "license-manager:ListLicenseConfigurations",
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor4",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DescribeLoadBalancers",
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor5",
      "Effect" : "Allow",
      "Action" : "iam:ListInstanceProfiles",
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor6",
```

```
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AWSApplicationMigrationLaunchInstanceWithSsmRole",
        "arn:aws:iam::*:role/service-role/
AWSApplicationMigrationLaunchInstanceWithDrsRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "VisualEditor7",
      "Effect" : "Allow",
      "Action" : [
        "drs:DescribeSourceServers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor8",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
```

```
      "Sid" : "VisualEditor9",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListCommandInvocations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor10",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "VisualEditor11",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument",
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSDisasterRecovery-InstallDRAgentOnInstance",
        "arn:aws:ssm:*:*:document/AWSMigration-*"
      ],
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "VisualEditor12",
      "Effect" : "Allow",
      "Action" : [
        "drs:DisconnectSourceServer"
      ],
```

```
      "Resource" : "arn:aws:drs:*:*:source-server/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceConfiguredDR" : "false"
        }
      }
    },
    {
      "Sid" : "VisualEditor13",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:PutParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/ManagedByAWSApplicationMigrationService-
*"
    },
    {
      "Sid" : "VisualEditor14",
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor15",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution"
      ],
      "Resource" : "arn:aws:ssm:*:*:automation-execution/*"
    },
    {
      "Sid" : "VisualEditor16",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSDisasterRecovery-InstallDRAgentOnInstance",
```

```
        "arn:aws:ssm:*:*:document/AWSMigration-*"
      ]
    },
    {
      "Sid" : "VisualEditor17",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameters"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/ManagedByAWSApplicationMigrationService-
*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "VisualEditor18",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSMigration-*",
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:automation-definition/AWSMigration-*:$DEFAULT"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "mgn.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "VisualEditor19",
      "Effect" : "Allow",
      "Action" : "ssm:ListCommands",
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "ssm.amazonaws.com"
        }
      }
```

```
    },
    {
      "Sid" : "VisualEditor20",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeParameters"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSApplicationMigrationMGHAccess

説明: このポリシーにより、 AWS Application Migration Service (MGN) は、MGN を使用して移行されるサーバーの進行状況に関するメタデータを AWS Migration Hub (MGH) に送信できます。MGN は、このポリシーがアタッチされた IAM ロールを自動的に作成し、このロールを引き受けます。IAM ユーザーまたはロールにこのポリシーをアタッチすることはおすすめしません。

`AWSApplicationMigrationMGHAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSApplicationMigrationMGHAccess` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2021 年 4 月 7 日 07:10 UTC
- 編集日時: 2021 年 4 月 7 日 07:10 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationMGHAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:AssociateCreatedArtifact",
        "mgh:CreateProgressUpdateStream",
        "mgh:DisassociateCreatedArtifact",
        "mgh:GetHomeRegion",
        "mgh:ImportMigrationTask",
        "mgh:NotifyMigrationTaskState",
        "mgh:PutResourceAttributes"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSApplicationMigrationNetworkMigrationCustomResource

説明: ネットワーク移行カスタムリソースのアクセス許可を提供します

AWSApplicationMigrationNetworkMigrationCustomResource は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSApplicationMigrationNetworkMigrationCustomResource をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 11 月 5 日 11:34 UTC
- 編集日時: 2025 年 11 月 5 日 11:34 UTC
- ARN: arn:aws:iam::aws:policy/AWSApplicationMigrationNetworkMigrationCustomResource

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ModifyTGW",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyTransitGateway"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:transit-gateway/*",
        "arn:aws:ec2:*:*:transit-gateway-route-table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSApplicationMigrationNetworkMigrationMultiAccount

説明: CloudFormation を介した VMware から AWS ネットワークインフラストラクチャへの移行を自動化するアクセス許可を提供します

`AWSApplicationMigrationNetworkMigrationMultiAccount` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに
AWSApplicationMigrationNetworkMigrationMultiAccount をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 11 月 10 日 09:04 UTC
- 編集日時: 2025 年 11 月 10 日 09:04 UTC
- ARN: arn:aws:iam::aws:policy/
  AWSApplicationMigrationNetworkMigrationMultiAccount

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2CFNReadonlyPrefixList",
      "Effect" : "Allow",
      "Action" : [
        "ec2:GetManagedPrefixListEntries"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:prefix-list/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "NetworkAnalyzer",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CreatePermissionsByCFNNACL",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ReplaceNetworkAclAssociation"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-acl/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreatePermissionsByCFNNACLSN",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ReplaceNetworkAclAssociation"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "EC2CFNReadonly",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeHosts",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeNetworkInsightsAnalyses",
        "ec2:DescribeNetworkInsightsPaths",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayPeeringAttachments",
```

```
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetTransitGatewayRouteTableAssociations",
        "ec2:GetTransitGatewayRouteTablePropagations"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "MGNCFNDescribe",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/Nmd*"
    },
    {
      "Sid" : "CFNCreate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/Nmd*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService",
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
```

```
        }
      }
    },
    {
      "Sid" : "CFNOperations",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DeleteStack",
        "cloudformation:UpdateStack",
        "cloudformation:UpdateTerminationProtection",
        "cloudformation:DescribeStackResources",
        "cloudformation:GetTemplateSummary",
        "cloudformation:ListStackResources",
        "cloudformation:DescribeStackEvents"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/Nmd*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "CFNProvision",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:elastic-ip/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "AnalyzerEC2PutResourcePolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:PutResourcePolicy"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "AnalyzerEC2ResourceOperations",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:security-group-rule/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "AnalyzerEC2ResourceSgTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
```

```
      "Sid" : "AnalyzerEC2RequestSgTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:security-group-rule/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "AnalyzerEC2SecurityGroupTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:security-group-rule/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
          "ec2:CreateAction" : [
            "CreateSecurityGroup"
          ]
        }
      }
    },
    {
      "Sid" : "EC2TagCFNSG",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:security-group-rule/*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreatePermissionsByCFN",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreatePermissionsByResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkAcl",
        "ec2:CreateNetworkAclEntry",
        "ec2:CreateSubnet",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateNatGateway",
        "ec2:CreateTransitGatewayRouteTable",
        "ec2:CreateTransitGatewayVpcAttachment",
        "ec2:CreateTransitGatewayRoute",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInsightsPath"
```

```
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-acl/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:natgateway/*",
        "arn:aws:ec2:*:*:transit-gateway/*",
        "arn:aws:ec2:*:*:transit-gateway-route-table/*",
        "arn:aws:ec2:*:*:transit-gateway-attachment/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:network-insights-path/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:elastic-ip/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowCreateTGWVpcAttachmentSameOrg",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTransitGatewayVpcAttachment"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:transit-gateway/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:transit-gateway-attachment/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceOrgID" : "${aws:PrincipalOrgID}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "CFNProvisionNetworking",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateInternetGateway",
        "ec2:CreateVpc",
        "ec2:CreateTransitGateway"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:internet-gateway/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:transit-gateway/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "CreatePermissionsByRequestTagNetworking",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkAcl",
        "ec2:CreateSubnet",
        "ec2:CreateRouteTable"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-acl/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "CreatePermissionsByRequestTagRouting",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkAclEntry",
        "ec2:CreateRoute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-acl/*",
        "arn:aws:ec2:*:*:route-table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreatePermissionsByRequestTagNAT",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNatGateway"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:natgateway/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:elastic-ip/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "CreatePermissionsByRequestTagTransitGateway",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTransitGatewayRouteTable",
        "ec2:CreateTransitGatewayRoute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:transit-gateway/*",
        "arn:aws:ec2:*:*:transit-gateway-route-table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreatePermissionsByRequestTagTGWAttachment",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTransitGatewayVpcAttachment"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:transit-gateway/*",
        "arn:aws:ec2:*:*:transit-gateway-attachment/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
```

```
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreatePermissionsByRequestTagNetworkInterface",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "DeleteENI",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "CreatePermissionsByRequestTagInsights",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInsightsPath"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-insights-path/*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "EC2TagCFN",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:transit-gateway/*",
        "arn:aws:ec2:*:*:transit-gateway-policy-table/*",
        "arn:aws:ec2:*:*:transit-gateway-connect-peer/*",
        "arn:aws:ec2:*:*:transit-gateway-route-table/*",
        "arn:aws:ec2:*:*:transit-gateway-attachment/*",
        "arn:aws:ec2:*:*:internet-gateway/*",
        "arn:aws:ec2:*:*:natgateway/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-acl/*",
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:network-insights-path/*",
        "arn:aws:ec2:*:*:network-insights-access-scope-analysis/*",
        "arn:aws:ec2:*:*:network-insights-access-scope/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:elastic-ip/*",
        "arn:aws:ec2:*:*:network-insights-analysis/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
          "ec2:CreateAction" : [
            "CreateTransitGatewayVpcAttachment",
            "CreateTransitGatewayRouteTableAnnouncement",
            "CreateTransitGatewayRouteTable",
```

```
            "CreateTransitGatewayRoute",
            "CreateTransitGatewayPrefixListReference",
            "CreateTransitGatewayPolicyTable",
            "CreateTransitGatewayPeeringAttachment",
            "CreateTransitGatewayConnectPeer",
            "CreateTransitGatewayConnect",
            "CreateTransitGateway",
            "CreateInternetGateway",
            "CreateNatGateway",
            "CreateSubnet",
            "CreateNetworkAcl",
            "CreateRouteTable",
            "CreateNetworkInterface",
            "CreateNetworkInsightsPath",
            "CreateNetworkInsightsAccessScope",
            "CreateLaunchTemplate",
            "AllocateAddress",
            "StartNetworkInsightsAnalysis",
            "CreateVpc"
          ]
        }
      }
    },
    {
      "Sid" : "deployerWorkload",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameters"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/network-migration/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "putParameter",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ssm:PutParameter",
        "ssm:AddTagsToResource"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/network-migration/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "deleteParameter",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteParameter",
        "ssm:PutResourcePolicy",
        "ssm:DeleteResourcePolicy",
        "ssm:ListTagsForResource",
        "ssm:GetResourcePolicies"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/network-migration/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ramTAgReource",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ram:TagResource"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreateResourceShareTransitGateway",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "Bool" : {
          "ram:RequestedAllowsExternalPrincipals" : "false"
        }
      }
    },
    {
      "Sid" : "AssociateResourceShare",
      "Effect" : "Allow",
      "Action" : [
        "ram:AssociateResourceShare"
      ],
```

```
      "Resource" : "arn:aws:ram:*:*:resource-share/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService",
          "ram:RequestedResourceType" : [
            "ec2:TransitGateway",
            "ssm:Parameter"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreateResourceShareWithResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "ram:DeleteResourceShare",
        "ram:DisassociateResourceShare",
        "ram:UpdateResourceShare"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowGetResourceShares",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShares"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share/*"
    },
```

```
    {
      "Sid" : "CreateCustomResourceLogGroup",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/lambda/network-migration-modify-tgw*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreateCustomResourceLambda",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:TagResource"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:network-migration*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService",
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "GetCustomResource",
      "Effect" : "Allow",
```

```
      "Action" : [
        "lambda:GetFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:network-migration*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "OperationsCustomResourceLambda",
      "Effect" : "Allow",
      "Action" : [
        "lambda:AddPermission",
        "lambda:DeleteFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:network-migration*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreateRoleCustomResource",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:TagRole"
      ],
```

```
      "Resource" : "arn:aws:iam::*:role/Nmd*modifyTransitGateway*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PassGetRoleCustomResource",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/Nmd*modifyTransitGateway*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PassRoleCustomResource",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/Nmd*modifyTransitGateway*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        }
```

```
      }
    },
    {
      "Sid" : "OperationsRoleCustomResource",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:GetRolePolicy",
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : "arn:aws:iam::*:role/Nmd*modifyTransitGateway*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AttachCustomResourceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/Nmd*modifyTransitGateway*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        },
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole",
            "arn:aws:iam::aws:policy/
AWSApplicationMigrationNetworkMigrationCustomResource"
          ]
        },
        "ForAnyValue:StringEquals" : {
```

```
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "MGNCFNBasedResourcesProvision",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AcceptTransitGatewayVpcAttachment",
        "ec2:AssociateNatGatewayAddress",
        "ec2:AssociateRouteTable",
        "ec2:AssociateSubnetCidrBlock",
        "ec2:AssociateTransitGatewayRouteTable",
        "ec2:AssociateVpcCidrBlock",
        "ec2:AttachInternetGateway",
        "ec2:AttachVolume",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteInternetGateway",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions",
        "ec2:DeleteNatGateway",
        "ec2:DeleteNetworkAcl",
        "ec2:DeleteNetworkAclEntry",
        "ec2:DeleteNetworkInsightsAnalysis",
        "ec2:DeleteNetworkInsightsPath",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteSnapshot",
        "ec2:DeleteSubnet",
        "ec2:DeleteTransitGateway",
        "ec2:DeleteTransitGatewayRoute",
        "ec2:DeleteTransitGatewayRouteTable",
        "ec2:DeleteTransitGatewayVpcAttachment",
        "ec2:DeleteVolume",
        "ec2:DeleteVpc",
        "ec2:DetachInternetGateway",
        "ec2:DetachVolume",
        "ec2:DisableTransitGatewayRouteTablePropagation",
        "ec2:DisassociateNatGatewayAddress",
```

```
        "ec2:DisassociateRouteTable",
        "ec2:DisassociateTransitGatewayRouteTable",
        "ec2:EnableTransitGatewayRouteTablePropagation",
        "ec2:ModifyInstanceAttribute",
        "ec2:ModifyLaunchTemplate",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyTransitGateway",
        "ec2:ModifyTransitGatewayVpcAttachment",
        "ec2:ModifyVolume",
        "ec2:ModifyVpcAttribute",
        "ec2:RejectTransitGatewayVpcAttachment",
        "ec2:ReleaseAddress",
        "ec2:ReplaceNetworkAclAssociation",
        "ec2:ReplaceNetworkAclEntry",
        "ec2:ReplaceRoute",
        "ec2:ReplaceTransitGatewayRoute",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:SearchTransitGatewayRoutes",
        "ec2:StartNetworkInsightsAnalysis"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:transit-gateway/*",
        "arn:aws:ec2:*:*:transit-gateway-policy-table/*",
        "arn:aws:ec2:*:*:transit-gateway-connect-peer/*",
        "arn:aws:ec2:*:*:transit-gateway-route-table/*",
        "arn:aws:ec2:*:*:transit-gateway-attachment/*",
        "arn:aws:ec2:*:*:internet-gateway/*",
        "arn:aws:ec2:*:*:natgateway/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-acl/*",
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:network-insights-path/*",
        "arn:aws:ec2:*:*:network-insights-access-scope-analysis/*",
        "arn:aws:ec2:*:*:network-insights-access-scope/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:elastic-ip/*",
        "arn:aws:ec2:*:*:network-insights-analysis/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:security-group/*",
```

```
        "arn:aws:ec2:*:*:security-group-rule/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AnalyzerENIResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSApplicationMigrationReadOnlyAccess

説明: このポリシーは、Application Migration Service (MGN) のすべての読み取り専用パブリック APIs と、MGN コンソールを完全に読み取り専用で使用するために必要な他の AWS サービスの一部の読み取り専用 APIs へのアクセス許可を提供します。このポリシーを IAM ユーザーまたはロールにアタッチします。

`AWSApplicationMigrationReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSApplicationMigrationReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 4 月 7 日 07:15 UTC
- 編集日時: 2023 年 3 月 20 日 08:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSApplicationMigrationReplicationServerPolicy

説明: このポリシーは、Application Migration Service によって起動される EC2 インスタンスである Application Migration Service (MGN) レプリケーションサーバーが MGN サービスと通信し、 に EBS スナップショットを作成することを許可します AWS アカウント。このポリシーを含む IAM ロールは、アプリケーション移行サービスによって MGN レプリケーションサーバーに (EC2 インスタンスプロファイルとして) アタッチされます。MGN レプリケーションサーバーは、必要に応じて MGN によって自動的に起動および終了されます。MGN レプリケーションサーバーは、MGN を使用して管理される移行プロセスの一環として AWS、外部サーバーから へのデータレプリケーションを容易にするために使用されます。IAM ユーザーまたはロールにこのポリシーをアタッチすることはおすすめしません。

`AWSApplicationMigrationReplicationServerPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSApplicationMigrationReplicationServerPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2021 年 4 月 7 日 07:21 UTC
- 編集日時: 2021 年 4 月 7 日 07:21 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationReplicationServerPolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSApplicationMigrationServiceEc2InstancePolicy

説明: このポリシーでは、 AWS アプリケーション移行サービス (AWS MGN) が EC2 (クロスリージョンまたはクロス AZ) で実行されるソースサーバーを移行するために使用する AWS レプリケーションエージェントをインストールして使用できます。このポリシーを含む IAM ロールは、EC2 インスタンスに (EC2 インスタンスプロファイルとして) アタッチする必要があります。

AWSApplicationMigrationServiceEc2InstancePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSApplicationMigrationServiceEc2InstancePolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 8 月 22 日 13:19 UTC
- 編集日時: 2024 年 1 月 3 日 14:19 UTC
- ARN: arn:aws:iam::aws:policy/AWSApplicationMigrationServiceEc2InstancePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSApplicationMigrationServiceRolePolicy

説明: AWS アプリケーション移行サービスがユーザーに代わって AWS リソースを作成および管理できるようにします。

AWSApplicationMigrationServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 4 月 7 日 06:43 UTC
- 編集日時: 2025 年 3 月 16 日 10:37 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationMigrationServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "mgn:ListTagsForResource",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "kms:ListRetirableGrants",
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "mgh:AssociateCreatedArtifact",
        "mgh:CreateProgressUpdateStream",
        "mgh:DisassociateCreatedArtifact",
        "mgh:GetHomeRegion",
        "mgh:ImportMigrationTask",
        "mgh:NotifyMigrationTaskState",
        "mgh:PutResourceAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:GetEbsDefaultKmsKeyId",
        "ec2:GetEbsEncryptionByDefault"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount"
      ],
      "Resource" : "arn:aws:organizations::*:account/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
```

```
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RegisterImage",
        "ec2:DeregisterImage"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:DeleteVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:GetConsoleOutput",
        "ec2:GetConsoleScreenshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
```

```
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
```

```
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AWSApplicationMigrationReplicationServerRole",
        "arn:aws:iam::*:role/service-role/AWSApplicationMigrationConversionServerRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateLaunchTemplate",
            "CreateSecurityGroup",
            "CreateVolume",
            "CreateSnapshot",
            "RunInstances"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSApplicationMigrationSSMAccess

説明: このポリシーは、アプリケーション移行サービス (MGN) を使用してカスタム移行後コマンド SSM ドキュメントを実行するために必要な Amazon SSM オペレーションへのアクセスを提供します。このポリシーを IAM ユーザーまたはロールにアタッチします。

`AWSApplicationMigrationSSMAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSApplicationMigrationSSMAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 11 月 27 日 9:29 UTC
- 編集日時: 2025 年 7 月 2 日 18:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationSSMAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetCommandInvocation",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:DescribeDocument",
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/*",
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:automation-definition/*:*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
```

```
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListDocuments"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListDocumentVersions",
        "ssm:GetDocument"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSApplicationMigrationVCenterClientPolicy

説明: このポリシーは、外部サーバーを移行するために AWS Application Migration Service (MGN) で使用される AWS VCenter クライアントのインストールと使用を許可します AWS。このポリシーを、 AWS VCenter クライアントのインストール時に指定した認証情報を持つ IAM ユーザーまたはロールにアタッチします。

AWSApplicationMigrationVCenterClientPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSApplicationMigrationVCenterClientPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 11 月 8 日 12:53 UTC
- 編集日時: 2021 年 11 月 8 日 12:53 UTC
- ARN: arn:aws:iam::aws:policy/AWSApplicationMigrationVCenterClientPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSAppMeshEnvoyAccess

説明: 仮想化ノード設定にアクセスするための App Mesh Envoy ポリシー。

AWSAppMeshEnvoyAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSAppMeshEnvoyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 7 月 3 日 21:29 UTC

- 編集日時: 2019 年 7 月 3 日 21:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppMeshEnvoyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSAppMeshFullAccess

説明: AWS App Mesh APIs とマネジメントコンソールへのフルアクセスを提供します。

`AWSAppMeshFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSAppMeshFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 4 月 16 日 17:50 UTC
- 編集日時: 2021 年 1 月 7 日 19:54 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppMeshFullAccess

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSAppMeshPreviewEnvoyAccess

説明: 仮想化ノード設定にアクセスするための App Mesh Preview Envoy ポリシー。

AWSAppMeshPreviewEnvoyAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSAppMeshPreviewEnvoyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 8 月 5 日 23:32 UTC
- 編集日時: 2019 年 8 月 5 日 23:32 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppMeshPreviewEnvoyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appmesh-preview:StreamAggregatedResources"
      ],
```

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSAppMeshPreviewServiceRolePolicy

説明: AWS App Mesh が使用または管理する AWS のサービス およびリソースへのアクセスを有効にします

AWSAppMeshPreviewServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 6 月 19 日 19:07 UTC
- 編集日時: 2019 年 8 月 21 日 21:06 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSAppMeshPreviewServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudMapServiceDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DiscoverInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ACMCertificateVerification",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSAppMeshReadOnly

説明: AWS App Mesh APIs とマネジメントコンソールへの読み取り専用アクセスを提供します。

AWSAppMeshReadOnly は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSAppMeshReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 4 月 16 日 17:51 UTC
- 編集日時: 2021 年 1 月 7 日 19:53 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppMeshReadOnly

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSAppMeshServiceRolePolicy

説明: AWS AppMesh が使用または管理する AWS のサービス および リソースへのアクセスを有効にします

AWSAppMeshServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 6 月 3 日 18:30 UTC
- 編集日時: 2023 年 10 月 10 日 16:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAppMeshServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudMapServiceDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DiscoverInstances",
        "servicediscovery:DiscoverInstancesRevision"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ACMCertificateVerification",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSAppRunnerFullAccess

説明: すべての App Runner アクションに対するアクセス許可を付与します。

AWSAppRunnerFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSAppRunnerFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 1 月 11 日 04:02 UTC
- 編集日時: 2022 年 1 月 11 日 04:02 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppRunnerFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSAppRunnerReadOnlyAccess

説明: App Runner リソースの詳細をリスト化および閲覧するアクセス許可を付与します。

AWSAppRunnerReadOnlyAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSAppRunnerReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 2 月 24 日 21:24 UTC
- 編集日時: 2022 年 2 月 24 日 21:24 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppRunnerReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する

- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSAppRunnerServicePolicyForECRAccess

説明: お客様のアカウントの Amazon ECR リソースに読み取りアクセス許可を付与する AWS App Runner サービスポリシー。App Runner サービスを作成または更新するときに App Runner に渡されるロールで使用してください。

AWSAppRunnerServicePolicyForECRAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSAppRunnerServicePolicyForECRAccess をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2021 年 5 月 14 日 19:17 UTC
- 編集日時: 2021 年 5 月 14 日 19:17 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSAppRunnerServicePolicyForECRAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "ecr:DescribeImages",
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSAppSyncAdministrator

説明: AppSync サービスへの管理者アクセスを提供しますが、コンソール経由でアクセスするには不十分です。

`AWSAppSyncAdministrator` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSAppSyncAdministrator` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 3 月 20 日 21:20 UTC
- 編集日時: 2019 年 11 月 4 日 19:23 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSAppSyncInvokeFullAccess

説明: コンソール経由あるいは単独での、AppSync サービスに対する呼び出しフルアクセスを提供

`AWSAppSyncInvokeFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSAppSyncInvokeFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 3 月 20 日 21:21 UTC
- 編集日時: 2018 年 3 月 20 日 21:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppSyncInvokeFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appsync:GraphQL",
        "appsync:GetGraphqlApi",
        "appsync:ListGraphqlApis",
        "appsync:ListApiKeys"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSAppSyncPushToCloudWatchLogs

説明: AppSync がユーザーの CloudWatch アカウントにログをプッシュできるようにします。

AWSAppSyncPushToCloudWatchLogs は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSAppSyncPushToCloudWatchLogs をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2018 年 4 月 9 日 19:38 UTC
- 編集日時: 2018 年 4 月 9 日 19:38 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSAppSyncPushToCloudWatchLogs

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する

- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSAppSyncSchemaAuthor

説明: スキーマの作成、更新、クエリを行うためのアクセスを提供します。

AWSAppSyncSchemaAuthor は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSAppSyncSchemaAuthor をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 3 月 20 日 21:21 UTC
- 編集日時: 2023 年 2 月 1 日 18:36 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppSyncSchemaAuthor

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSAppSyncServiceRolePolicy

説明: AppSync が使用または管理する AWS サービスとリソースへのアクセスを有効にします

AWSAppSyncServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 1 月 21 日 19:56 UTC
- 編集日時: 2020 年 1 月 21 日 19:56 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSAppSyncServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingTargets",
        "xray:GetSamplingRules",
        "xray:GetSamplingStatisticSummaries"
```

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSArtifactAccountSync

説明: AWS Organizations のオペレーションへの AWS アーティファクトの読み取り専用アクセスを許可します。

AWSArtifactAccountSync は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSArtifactAccountSync をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2018 年 4 月 10 日 23:04 UTC
- 編集日時: 2018 年 4 月 10 日 23:04 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSArtifactAccountSync

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSArtifactAgreementsFullAccess

説明: このポリシーは、 AWS アーティファクト契約を一覧表示、ダウンロード、承諾、終了するための完全なアクセス許可を付与します。また、Organization サービスで AWS サービスアクセスを一覧表示して有効にし、組織の詳細を記述するアクセス許可も含まれています。さらに、このポリシーは、必要なサービスにリンクされたロールが存在するかどうかを確認し、存在しない場合はロールを作成する機能を提供します。

AWSArtifactAgreementsFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSArtifactAgreementsFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 11 月 22 日 19:36 UTC
- 編集日時: 2025 年 10 月 16 日 20:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSArtifactAgreementsFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ListAgreementActions",
      "Effect" : "Allow",
      "Action" : [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSAgreementActions",
      "Effect" : "Allow",
      "Action" : [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource" : "arn:aws:artifact:::agreement/*"
    },
```

```
    {
      "Sid" : "CustomerAgreementActions",
      "Effect" : "Allow",
      "Action" : [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource" : "arn:aws:artifact::*:customer-agreement/*"
    },
    {
      "Sid" : "CreateServiceLinkedRoleForOrganizationsIntegration",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "artifact.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "GetRoleToCheckForRoleExistence",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact"
    },
    {
      "Sid" : "EnableServiceTrust",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "EnableServiceTrustForArtifact",
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "aws-artifact-account-sync.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSArtifactAgreementsReadOnlyAccess

説明: このポリシーは、 AWS アーティファクトサービス契約を一覧表示し、承認された契約をダウンロードするための読み取り専用アクセス権を付与します。また、組織の詳細を一覧表示および説明するアクセス許可も含まれています。さらに、このポリシーは、必要なサービスにリンクされたロールが存在するかどうかを確認する機能を提供します。

AWSArtifactAgreementsReadOnlyAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSArtifactAgreementsReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 11 月 22 日 19:36 UTC
- 編集日時: 2024 年 11 月 22 日 19:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSArtifactAgreementsReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ListAgreementsActions",
      "Effect" : "Allow",
      "Action" : [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetCustomerAgreementActions",
      "Effect" : "Allow",
      "Action" : [
        "artifact:GetCustomerAgreement"
      ],
      "Resource" : "arn:aws:artifact::*:customer-agreement/*"
    },
    {
      "Sid" : "AWSOrganizationActions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSArtifactReportsReadOnlyAccess

説明: AWS Artifact サービスレポートへの読み取り専用アクセスを提供します。

`AWSArtifactReportsReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSArtifactReportsReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2024 年 1 月 2 日 22:42 UTC
- 編集日時: 2025 年 12 月 16 日 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSArtifactReportsReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ArtifactReportActions",
      "Effect" : "Allow",
      "Action" : [
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports",
        "artifact:ListReportVersions"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSArtifactServiceRolePolicy

説明: AWS Artifact が AWS Organizations サービスを介して組織に関する情報を収集できるようにします。

AWSArtifactServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 8 月 21 日 20:27 UTC
- 編集日時: 2023 年 8 月 21 日 20:27 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSArtifactServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSAuditManagerAdministratorAccess

説明: AWS Audit Manager の有効化または無効化、設定の更新、評価、コントロール、フレームワークの管理を行うための管理アクセスを提供します

AWSAuditManagerAdministratorAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSAuditManagerAdministratorAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 12 月 11 日 20:02 UTC
- 編集日時: 2024 年 5 月 15 日 23:46 UTC
- ARN: arn:aws:iam::aws:policy/AWSAuditManagerAdministratorAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSAuditManagerServiceRolePolicy

説明: AWS Audit Manager が使用または管理する AWS のサービス およびリソースへのアクセスを有効にします

`AWSAuditManagerServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 12 月 8 日 15:12 UTC
- 編集日時: 2024 年 9 月 24 日 23:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAuditManagerServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v10 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:GetAccountConfiguration",
        "acm:ListCertificates",
        "autoscaling:DescribeAutoScalingGroups",
        "backup:ListBackupPlans",
        "backup:ListRecoveryPointsByResource",
        "bedrock:GetCustomModel",
        "bedrock:GetFoundationModel",
        "bedrock:GetModelCustomizationJob",
        "bedrock:GetModelInvocationLoggingConfiguration",
        "bedrock:ListCustomModels",
        "bedrock:ListFoundationModels",
        "bedrock:ListGuardrails",
        "bedrock:ListModelCustomizationJobs",
        "cloudfront:GetDistribution",
        "cloudfront:GetDistributionConfig",
        "cloudfront:ListDistributions",
        "cloudtrail:GetTrail",
        "cloudtrail:ListTrails",
        "cloudtrail:DescribeTrails",
        "cloudtrail:LookupEvents",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cognito-idp:DescribeUserPool",
        "config:DescribeConfigRules",
        "config:DescribeDeliveryChannels",
        "config:ListDiscoveredResources",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualGateways",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeBackup",
        "dynamodb:DescribeTableReplicaAutoScaling",
        "dynamodb:DescribeTable",
        "dynamodb:ListBackups",
```

```
        "dynamodb:ListGlobalTables",
        "dynamodb:ListTables",
        "ec2:DescribeInstanceCreditSpecifications",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeVpcEndpointConnections",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:GetLaunchTemplateData",
        "ec2:DescribeAddresses",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
        "ec2:DescribeLocalGateways",
        "ec2:DescribeLocalGatewayVirtualInterfaces",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetEbsDefaultKmsKeyId",
        "ec2:GetEbsEncryptionByDefault",
        "ecs:DescribeClusters",
        "eks:DescribeAddonVersions",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeServiceUpdates",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeFileSystems",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeSslPolicies",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListSecurityConfigurations",
        "events:DescribeRule",
        "events:ListConnections",
```

```
        "events:ListEventBuses",
        "events:ListEventSources",
        "events:ListRules",
        "firehose:ListDeliveryStreams",
        "fsx:DescribeFileSystems",
        "guardduty:ListDetectors",
        "iam:GenerateCredentialReport",
        "iam:GetAccountAuthorizationDetails",
        "iam:GetAccessKeyLastUsed",
        "iam:GetCredentialReport",
        "iam:GetGroupPolicy",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRolePolicy",
        "iam:GetUser",
        "iam:GetUserPolicy",
        "iam:GetAccountPasswordPolicy",
        "iam:GetAccountSummary",
        "iam:ListAttachedGroupPolicies",
        "iam:ListAttachedUserPolicies",
        "iam:ListEntitiesForPolicy",
        "iam:ListGroupsForUser",
        "iam:ListGroupPolicies",
        "iam:ListGroups",
        "iam:ListOpenIdConnectProviders",
        "iam:ListPolicies",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListSamlProviders",
        "iam:ListUserPolicies",
        "iam:ListUsers",
        "iam:ListVirtualMFADevices",
        "iam:ListPolicyVersions",
        "iam:ListAccessKeys",
        "iam:ListAttachedRolePolicies",
        "iam:ListMfaDeviceTags",
        "iam:ListMfaDevices",
        "kafka:ListClusters",
        "kafka:ListKafkaVersions",
        "kinesis:ListStreams",
        "kms:DescribeKey",
        "kms:GetKeyPolicy",
        "kms:GetKeyRotationStatus",
        "kms:ListGrants",
```

```
        "kms:ListKeyPolicies",
        "kms:ListKeys",
        "lambda:ListFunctions",
        "license-manager:ListAssociationsForLicenseConfiguration",
        "license-manager:ListLicenseConfigurations",
        "license-manager:ListUsageForLicenseConfiguration",
        "logs:DescribeDestinations",
        "logs:DescribeExportTasks",
        "logs:DescribeLogGroups",
        "logs:DescribeMetricFilters",
        "logs:DescribeResourcePolicies",
        "logs:FilterLogEvents",
        "logs:GetDataProtectionPolicy",
        "es:DescribeDomains",
        "es:DescribeDomain",
        "es:DescribeDomainConfig",
        "es:ListDomainNames",
        "organizations:DescribeOrganization",
        "organizations:DescribePolicy",
        "rds:DescribeCertificates",
        "rds:DescribeDBClusterEndpoints",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBInstances",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstanceAutomatedBackups",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeLoggingStatus",
        "route53:GetQueryLoggingConfig",
        "sagemaker:DescribeAlgorithm",
        "sagemaker:DescribeFlowDefinition",
        "sagemaker:DescribeHumanTaskUi",
        "sagemaker:DescribeModelBiasJobDefinition",
        "sagemaker:DescribeModelCard",
        "sagemaker:DescribeModelQualityJobDefinition",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeLabelingJob",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:DescribeUserProfile",
        "sagemaker:ListAlgorithms",
```

```
        "sagemaker:ListDomains",
        "sagemaker:ListEndpoints",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListFlowDefinitions",
        "sagemaker:ListHumanTaskUis",
        "sagemaker:ListLabelingJobs",
        "sagemaker:ListModels",
        "sagemaker:ListModelBiasJobDefinitions",
        "sagemaker:ListModelCards",
        "sagemaker:ListModelQualityJobDefinitions",
        "sagemaker:ListMonitoringAlerts",
        "sagemaker:ListMonitoringSchedules",
        "sagemaker:ListTrainingJobs",
        "sagemaker:ListUserProfiles",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketVersioning",
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:ListAllMyBuckets",
        "secretsmanager:DescribeSecret",
        "secretsmanager:ListSecrets",
        "securityhub:DescribeStandards",
        "sns:ListTagsForResource",
        "sns:ListTopics",
        "sqs:ListQueues",
        "waf-regional:GetRule",
        "waf-regional:GetWebAcl",
        "waf:GetRule",
        "waf:GetRuleGroup",
        "waf:ListActivatedRulesInRuleGroup",
        "waf:ListWebAcls",
        "wafv2:ListWebAcls",
        "waf-regional:GetLoggingConfiguration",
        "waf-regional:ListRuleGroups",
        "waf-regional:ListSubscribedRuleGroups",
        "waf-regional:ListWebACLs",
        "waf-regional:ListRules",
        "waf:ListRuleGroups",
        "waf:ListRules"
      ],
      "Resource" : "*",
      "Sid" : "APIsAccess"
    },
    {
```

```
      "Sid" : "S3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketAcl",
        "s3:GetBucketLogging",
        "s3:GetBucketOwnershipControls",
        "s3:GetBucketPolicy",
        "s3:GetBucketTagging"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : [
            "${aws:PrincipalAccount}"
          ]
        }
      }
    },
    {
      "Sid" : "APIGatewayAccess",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/restapis/*/stages"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : [
            "${aws:PrincipalAccount}"
          ]
        }
      }
    },
    {
      "Sid" : "CreateEventsAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver",
```

```
      "Condition" : {
        "StringEquals" : {
          "events:detail-type" : "Security Hub Findings - Imported"
        },
        "Null" : {
          "events:source" : "false"
        },
        "ForAllValues:StringEquals" : {
          "events:source" : [
            "aws.securityhub"
          ]
        }
      }
    },
    {
      "Sid" : "EventsAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:EnableRule",
        "events:DisableRule",
        "events:ListTargetsByRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSAutoScalingPlansEC2AutoScalingPolicy

説明: スケーリングプラン内の AWS Auto Scaling グループのキャパシティを定期的に予測し、スケジュールされたスケーリングアクションを生成するアクセス許可を Auto Scaling に付与するポリシー

AWSAutoScalingPlansEC2AutoScalingPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 8 月 23 日 22:46 UTC
- 編集日時: 2018 年 8 月 23 日 22:46 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSAutoScalingPlansEC2AutoScalingPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeScheduledActions",
        "autoscaling:BatchPutScheduledUpdateGroupAction",
        "autoscaling:BatchDeleteScheduledAction"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSBackupAuditAccess

説明: このポリシーは、 AWS バックアップリソースとアクティビティに対する期待を定義するコントロールとフレームワークを作成し、定義されたコントロールとフレームワークに対して AWS バックアップリソースとアクティビティを監査するアクセス許可をユーザーに付与します。このポリシーは、Config AWS および同様のサービスにアクセス許可を付与して、監査を実行するユーザーの期待を記述します。このポリシーは、S3 および同様のサービスに監査レポートを配信するアクセス権限も付与し、ユーザーは監査レポートを見つけて開くことができます。

`AWSBackupAuditAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSBackupAuditAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 8 月 24 日 01:02 UTC
- 編集日時: 2023 年 4 月 10 日 21:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupAuditAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSBackupDataTransferAccess

説明: このポリシーにより、 AWS Backint エージェントは AWS Backup Storage プレーンを使用してバックアップデータ転送を完了できます。このポリシーを Backint エージェントで SAP HANA を実行している EC2 インスタンスが引き受けるロールにアタッチします。

`AWSBackupDataTransferAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSBackupDataTransferAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 11 月 10 日 22:48 UTC
- 編集日時: 2022 年 11 月 10 日 22:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupDataTransferAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSBackupFullAccess

説明: このポリシーはバックアップ管理者を対象としており、 AWS バックアッププランの作成または編集、バックアッププランへの AWS リソースの割り当て、バックアップの削除、バックアップの復元など、バックアップオペレーションへのフルアクセスを許可します。

AWSBackupFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSBackupFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 11 月 18 日 22:21 UTC
- 編集日時: 2025 年 11 月 20 日 03:34 UTC
- ARN: arn:aws:iam::aws:policy/AWSBackupFullAccess

ポリシーのバージョン

ポリシーのバージョン: v22 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AwsBackupAllAccessPermissions",
      "Effect" : "Allow",
      "Action" : "backup:*",
      "Resource" : "*"
    },
    {
      "Sid" : "AwsBackupStorageAllAccessPermissions",
```

```
      "Effect" : "Allow",
      "Action" : "backup-storage:*",
      "Resource" : "*"
    },
    {
      "Sid" : "RdsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBSnapshots",
        "rds:ListTagsForResource",
        "rds:DescribeDBInstances",
        "rds:describeDBEngineVersions",
        "rds:describeOptionGroups",
        "rds:describeOrderableDBInstanceOptions",
        "rds:describeDBSubnetGroups",
        "rds:describeDBClusterSnapshots",
        "rds:describeDBClusters",
        "rds:describeDBParameterGroups",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBInstanceAutomatedBackups",
        "rds:DescribeDBClusterAutomatedBackups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RdsDeletePermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:DeleteDBSnapshot",
        "rds:DeleteDBClusterSnapshot"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DynamoDbPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "dynamodb:ListBackups",
        "dynamodb:ListTables"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DynamoDbDeleteBackupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DeleteBackup"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "EfsFileSystemPermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeFilesystems"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*"
    },
    {
      "Sid" : "Ec2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes",
        "ec2:describeAvailabilityZones",
        "ec2:DescribeVpcs",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeImages",
        "ec2:DescribeSubnets",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeVpcEndpoints",
```

```
        "ec2:DescribeAddresses"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Ec2DeletePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot",
        "ec2:DeregisterImage"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ResourceGroupTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetTagKeys",
        "tag:GetTagValues",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "StorageGatewayVolumePermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:DescribeCachediSCSIVolumes",
        "storagegateway:DescribeStorediSCSIVolumes"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*/volume/*"
    },
    {
      "Sid" : "StorageGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:ListGateways"
```

```
      ],
      "Resource" : "arn:aws:storagegateway:*:*:*"
    },
    {
      "Sid" : "StorageGatewayGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:DescribeGatewayInformation",
        "storagegateway:ListLocalDisks"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*"
    },
    {
      "Sid" : "StorageGatewayGatewayStarPermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:ListVolumes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IamRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "iam:GetRole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IamPassRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/*AwsBackup*",
        "arn:aws:iam::*:role/*AWSBackup*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "backup.amazonaws.com",
            "restore-testing.backup.amazonaws.com"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "AwsOrganizationsPermissions",
      "Effect" : "Allow",
      "Action" : "organizations:DescribeOrganization",
      "Resource" : "*"
    },
    {
      "Sid" : "KmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KmsCreateGrantPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:backup:backup-vault"
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        },
        "StringLike" : {
          "kms:ViaService" : "backup.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SystemManagerCommandPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CancelCommand",
        "ssm:GetCommandInvocation"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SystemManagerSendCommandPermissions",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSEC2-CreateVssSnapshot",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Sid" : "FsxPermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeFileSystems",
        "fsx:DescribeBackups",
        "fsx:DescribeVolumes",
        "fsx:DescribeStorageVirtualMachines"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "FsxDeletePermissions",
      "Effect" : "Allow",
      "Action" : "fsx:DeleteBackup",
      "Resource" : "arn:aws:fsx:*:*:backup/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DirectoryServicePermissions",
      "Effect" : "Allow",
      "Action" : "ds:DescribeDirectories",
      "Resource" : "*"
    },
    {
      "Sid" : "IamCreateServiceLinkedRolePermissions",
```

```
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "backup.amazonaws.com",
            "restore-testing.backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "BackupGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:AssociateGatewayToServer",
        "backup-gateway:CreateGateway",
        "backup-gateway:DeleteGateway",
        "backup-gateway:DeleteHypervisor",
        "backup-gateway:DisassociateGatewayFromServer",
        "backup-gateway:ImportHypervisorConfiguration",
        "backup-gateway:ListGateways",
        "backup-gateway:ListHypervisors",
        "backup-gateway:ListTagsForResource",
        "backup-gateway:ListVirtualMachines",
        "backup-gateway:PutMaintenanceStartTime",
        "backup-gateway:TagResource",
        "backup-gateway:TestHypervisorConfiguration",
        "backup-gateway:UntagResource",
        "backup-gateway:UpdateGatewayInformation",
        "backup-gateway:UpdateHypervisor"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BackupGatewayHypervisorPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:GetHypervisor",
        "backup-gateway:GetHypervisorPropertyMappings",
        "backup-gateway:PutHypervisorPropertyMappings",
        "backup-gateway:StartVirtualMachinesMetadataSync"
      ],
```

```
      "Resource" : "arn:aws:backup-gateway:*:*:hypervisor/*"
    },
    {
      "Sid" : "BackupGatewayVirtualMachinePermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:GetVirtualMachine"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:vm/*"
    },
    {
      "Sid" : "BackupGatewayGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:GetBandwidthRateLimitSchedule",
        "backup-gateway:GetGateway",
        "backup-gateway:PutBandwidthRateLimitSchedule"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:gateway/*"
    },
    {
      "Sid" : "CloudWatchPermissions",
      "Effect" : "Allow",
      "Action" : "cloudwatch:GetMetricData",
      "Resource" : "*"
    },
    {
      "Sid" : "TimestreamDatabasePermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:ListTables",
        "timestream:ListDatabases"
      ],
      "Resource" : [
        "arn:aws:timestream:*:*:database/*"
      ]
    },
    {
      "Sid" : "TimestreamPermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:DescribeEndpoints"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "S3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "RedshiftResourcesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSubnetGroups",
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeSnapshotSchedules"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:cluster:*",
        "arn:aws:redshift:*:*:subnetgroup:*",
        "arn:aws:redshift:*:*:snapshot:*/*",
        "arn:aws:redshift:*:*:snapshotschedule:*"
      ]
    },
    {
      "Sid" : "RedshiftPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeNodeConfigurationOptions",
        "redshift:DescribeOrderableClusterOptions",
        "redshift:DescribeClusterParameterGroups",
        "redshift:DescribeClusterTracks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftServerlessListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListSnapshots",
        "redshift-serverless:ListWorkgroups"
      ],
```

```
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "RedshiftServerlessGetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetSnapshot",
        "redshift-serverless:GetWorkgroup"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*",
        "arn:aws:redshift-serverless:*:*:workgroup/*",
        "arn:aws:redshift-serverless:*:*:snapshot/*"
      ]
    },
    {
      "Sid" : "RedshiftServerlessDeletetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:DeleteSnapshot"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:snapshot/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CloudFormationStackPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStacks"
      ],
```

```
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/*"
      ]
    },
    {
      "Sid" : "SystemsManagerForSapPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:GetOperation",
        "ssm-sap:ListDatabases",
        "ssm-sap:GetDatabase",
        "ssm-sap:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ResourceAccessManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShareAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DSQLDescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "dsql:GetCluster",
        "dsql:ListClusters",
        "dsql:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EKSClusterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "eks:ListClusters",
        "eks:ListTagsForResource",
        "eks:DescribeCluster"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/*"
    },
    {
```

```
      "Sid" : "IamPassRolePermissionsForGuardDuty",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/*AwsBackupGuardDuty*",
        "arn:aws:iam::*:role/*AWSBackupGuardDuty*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "malware-protection.guardduty.amazonaws.com"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync

説明: ユーザーに代わって仮想マシンのメタデータを同期するための Provides AWS BackupGateway アクセス許可

AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー

- 作成日時: 2022 年 12 月 15 日 19:43 UTC
- 編集日時: 2022 年 12 月 15 日 19:43 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSBackupGuardDutyRolePolicyForScans

説明: GuardDuty にマルウェアスキャンの AWS バックアップリカバリポイントを読み取るアクセス許可を付与します

AWSBackupGuardDutyRolePolicyForScans は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSBackupGuardDutyRolePolicyForScans をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 11 月 20 日 03:34 UTC
- 編集日時: 2025 年 11 月 20 日 03:34 UTC
- ARN: arn:aws:iam::aws:policy/AWSBackupGuardDutyRolePolicyForScans

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EBSDirectReadAPIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ebs:ListSnapshotBlocks",
        "ebs:ListChangedBlocks",
        "ebs:GetSnapshotBlock"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        },
        "StringLike" : {
          "aws:ResourceTag/aws:backup:source-resource" : "*"
        }
      }
    },
    {
      "Sid" : "CreateGrantForEncryptedVolumeCreation",
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:EncryptionContext:aws:guardduty:id" : "snap-*",
          "kms:ViaService" : [
            "guardduty.*.amazonaws.com",
            "backup.*.amazonaws.com"
          ]
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt",
            "CreateGrant",
            "GenerateDataKeyWithoutPlaintext",
            "ReEncryptFrom",
            "ReEncryptTo",
            "RetireGrant",
            "DescribeKey"
          ]
        },
```

```
        "Null" : {
          "kms:GrantOperations" : "false"
        }
      }
    },
    {
      "Sid" : "CreateGrantForReEncryptAndEBSDirect",
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:EncryptionContext:aws:ebs:id" : "snap-*",
          "kms:ViaService" : [
            "guardduty.*.amazonaws.com",
            "backup.*.amazonaws.com"
          ]
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt",
            "ReEncryptFrom",
            "ReEncryptTo",
            "RetireGrant",
            "DescribeKey"
          ]
        },
        "Null" : {
          "kms:GrantOperations" : "false"
        }
      }
    },
    {
      "Sid" : "DescribeKeyPermissions",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
      "Sid" : "EC2ReadAPIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ShareSnapshotPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        },
        "StringLike" : {
          "aws:ResourceTag/aws:backup:source-resource" : "*"
        }
      }
    },
    {
      "Sid" : "ShareSnapshotKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:EncryptionContext:aws:ebs:id" : [
            "vol-*",
            "snap-*"
          ],
          "kms:ViaService" : "ec2.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CreateBackupAccessPointPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:CreateBackupAccessPoint"
      ],
      "Resource" : "arn:aws:backup:*:*:recovery-point:*"
```

```
    },
    {
      "Sid" : "ReadAndDeleteBackupAccessPointPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:DescribeBackupAccessPoint",
        "backup:DeleteBackupAccessPoint"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BackupRecoveryPointApiPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:DescribeRecoveryPoint"
      ],
      "Resource" : "arn:aws:backup:*:*:recovery-point:*"
    },
    {
      "Sid" : "DecryptKMSEncryptedDataByAWSBackup",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:EncryptionContext:aws:backup:backup-vault" : "*",
          "kms:ViaService" : "backup.*.amazonaws.com"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSBackupOperatorAccess

説明: このポリシーは、バックアッププランへの AWS リソースの割り当て、オンデマンドバックアップの作成、バックアップの復元を行うアクセス許可をユーザーに付与します。このポリシーは、ユーザーがバックアッププランを作成、または編集したり、スケジュールされたバックアップを作成後に削除したりするためのアクセス許可は持っていません。

AWSBackupOperatorAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSBackupOperatorAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 11 月 18 日 22:23 UTC
- 編集日時: 2025 年 11 月 20 日 03:34 UTC
- ARN: arn:aws:iam::aws:policy/AWSBackupOperatorAccess

ポリシーのバージョン

ポリシーのバージョン: v20 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AwsBackupAllAccess",
      "Effect" : "Allow",
      "Action" : [
        "backup:Get*",
        "backup:List*",
        "backup:Describe*",
```

```
        "backup:CreateBackupSelection",
        "backup:DeleteBackupSelection",
        "backup:StartBackupJob",
        "backup:StartRestoreJob",
        "backup:StartCopyJob",
        "backup:StartScanJob"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RDSDescribeAccess",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBSnapshots",
        "rds:ListTagsForResource",
        "rds:DescribeDBInstances",
        "rds:describeDBEngineVersions",
        "rds:describeOptionGroups",
        "rds:describeOrderableDBInstanceOptions",
        "rds:describeDBSubnetGroups",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBInstanceAutomatedBackups",
        "rds:DescribeDBClusterAutomatedBackups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DynamoDBAccess",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListBackups",
        "dynamodb:ListTables"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EFSAccess",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeFilesystems"
      ],
```

```
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*"
    },
    {
      "Sid" : "EC2Access",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes",
        "ec2:describeAvailabilityZones",
        "ec2:DescribeVpcs",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeImages",
        "ec2:DescribeSubnets",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeAddresses"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TagReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetTagKeys",
        "tag:GetTagValues",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "StorageGatewaySCSIAccess",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:DescribeCachediSCSIVolumes",
        "storagegateway:DescribeStorediSCSIVolumes"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*/volume/*"
    },
    {
      "Sid" : "StorageGatewayReadAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "storagegateway:ListGateways"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:*"
    },
    {
      "Sid" : "StorageGatewayDiskReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:DescribeGatewayInformation",
        "storagegateway:ListLocalDisks"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*"
    },
    {
      "Sid" : "StorageGatewayVolumeReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:ListVolumes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "iam:GetRole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassRoleAccess",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/*AwsBackup*",
        "arn:aws:iam::*:role/*AWSBackup*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "backup.amazonaws.com"
        }
      }
```

```
    },
    {
      "Sid" : "OrganizationsAccess",
      "Effect" : "Allow",
      "Action" : "organizations:DescribeOrganization",
      "Resource" : "*"
    },
    {
      "Sid" : "SSMReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CancelCommand",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMComandAccess",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSEC2-CreateVssSnapshot",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Sid" : "FSXDescribeAccess",
      "Effect" : "Allow",
      "Action" : "fsx:DescribeBackups",
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    },
    {
      "Sid" : "FSxFileAccess",
      "Effect" : "Allow",
      "Action" : "fsx:DescribeFileSystems",
      "Resource" : "arn:aws:fsx:*:*:file-system/*"
    },
    {
      "Sid" : "FSxVolumeAccess",
      "Effect" : "Allow",
      "Action" : "fsx:DescribeVolumes",
      "Resource" : "arn:aws:fsx:*:*:volume/*/*"
    },
    {
```

```
      "Sid" : "FSxMachineAccess",
      "Effect" : "Allow",
      "Action" : "fsx:DescribeStorageVirtualMachines",
      "Resource" : "arn:aws:fsx:*:*:storage-virtual-machine/*/*"
    },
    {
      "Sid" : "DirectoryServiceAccess",
      "Effect" : "Allow",
      "Action" : "ds:DescribeDirectories",
      "Resource" : "*"
    },
    {
      "Sid" : "BackupGatewayListAccess",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:ListGateways",
        "backup-gateway:ListHypervisors",
        "backup-gateway:ListTagsForResource",
        "backup-gateway:ListVirtualMachines"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BackupGatewayHypervisorAccess",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:GetHypervisor",
        "backup-gateway:GetHypervisorPropertyMappings"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:hypervisor/*"
    },
    {
      "Sid" : "BackupGatewayMachineAccess",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:GetVirtualMachine"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:vm/*"
    },
    {
      "Sid" : "BackupGatewayAccess",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:GetBandwidthRateLimitSchedule",
```

```
        "backup-gateway:GetGateway"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:gateway/*"
    },
    {
      "Sid" : "CloudWatchAccess",
      "Effect" : "Allow",
      "Action" : "cloudwatch:GetMetricData",
      "Resource" : "*"
    },
    {
      "Sid" : "TimestreamListAccess",
      "Effect" : "Allow",
      "Action" : [
        "timestream:ListDatabases",
        "timestream:ListTables"
      ],
      "Resource" : [
        "arn:aws:timestream:*:*:database/*"
      ]
    },
    {
      "Sid" : "TimestreamDescribeAccess",
      "Effect" : "Allow",
      "Action" : [
        "timestream:DescribeEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3ListAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "RedshiftAccess",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSubnetGroups",
        "redshift:DescribeClusterSnapshots",
```

```
        "redshift:DescribeSnapshotSchedules"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:cluster:*",
        "arn:aws:redshift:*:*:subnetgroup:*",
        "arn:aws:redshift:*:*:snapshot:*/*",
        "arn:aws:redshift:*:*:snapshotschedule:*"
      ]
    },
    {
      "Sid" : "RedshiftOptionsAccess",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeNodeConfigurationOptions",
        "redshift:DescribeOrderableClusterOptions",
        "redshift:DescribeClusterParameterGroups",
        "redshift:DescribeClusterTracks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftServerlessListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListSnapshots",
        "redshift-serverless:ListWorkgroups"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "RedshiftServerlessGetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetSnapshot",
        "redshift-serverless:GetWorkgroup"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*",
        "arn:aws:redshift-serverless:*:*:workgroup/*",
        "arn:aws:redshift-serverless:*:*:snapshot/*"
```

```
      ]
    },
    {
      "Sid" : "CloudFormationAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStacks"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/*"
      ]
    },
    {
      "Sid" : "SAPAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:GetOperation",
        "ssm-sap:ListDatabases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SAPDatabaseAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:GetDatabase",
        "ssm-sap:ListTagsForResource"
      ],
      "Resource" : "arn:aws:ssm-sap:*:*:*"
    },
    {
      "Sid" : "RAMAccess",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShareAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DSQLDescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "dsql:GetCluster",
        "dsql:ListClusters",
```

```
        "dsql:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EKSClusterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "eks:ListClusters",
        "eks:ListTagsForResource",
        "eks:DescribeCluster"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/*"
    },
    {
      "Sid" : "IamPassRolePermissionsForGuardDuty",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/*AwsBackupGuardDuty*",
        "arn:aws:iam::*:role/*AWSBackupGuardDuty*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "malware-protection.guardduty.amazonaws.com"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSBackupOrganizationAdminAccess

説明: このポリシーは、クロスアカウントバックアップ管理を使用して組織のバックアップを管理するバックアップ管理者を対象としています。

AWSBackupOrganizationAdminAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSBackupOrganizationAdminAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 6 月 24 日 16:23 UTC
- 編集日時: 2022 年 11 月 18 日 18:26 UTC
- ARN: arn:aws:iam::aws:policy/AWSBackupOrganizationAdminAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSBackupRestoreAccessForSAPHANA

説明: Amazon EC2 で SAP HANA のバックアップを復元する AWS Backup アクセス許可を提供します

AWSBackupRestoreAccessForSAPHANA は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSBackupRestoreAccessForSAPHANA をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 11 月 10 日 22:43 UTC
- 編集日時: 2022 年 11 月 10 日 22:43 UTC
- ARN: arn:aws:iam::aws:policy/AWSBackupRestoreAccessForSAPHANA

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSBackupSearchOperatorAccess

説明: 検索オペレーターロールは、バックアップインデックスの作成、インデックスが作成されたバックアップメタデータの検索の作成にアクセスできます。このポリシーには、これらの検索演算子関数に必要なアクセス許可が含まれています。

AWSBackupSearchOperatorAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSBackupSearchOperatorAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2025 年 2 月 27 日 21:52 UTC
- 編集日時: 2025 年 3 月 25 日 19:52 UTC
- ARN: arn:aws:iam::aws:policy/AWSBackupSearchOperatorAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "StartSearchAndListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-search:StartSearchJob",
        "backup-search:ListSearchJobs",
        "backup-search:ListSearchResultExportJobs",
        "backup:ListIndexedRecoveryPointsForSearch"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BackupSearchRecoveryPointPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:SearchRecoveryPoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:backup:*:*:recovery-point:*"
      ]
    },
    {
      "Sid" : "SearchAndExportPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "backup-search:StartSearchResultExportJob",
        "backup-search:StopSearchJob",
        "backup-search:GetSearchJob",
        "backup-search:GetSearchResultExportJob",
        "backup-search:ListSearchJobResults",
        "backup-search:ListSearchJobBackups"
      ],
      "Resource" : [
        "arn:aws:backup-search:*:*:search-job/*",
        "arn:aws:backup-search:*:*:search-export-job/*"
      ]
    },
    {
      "Sid" : "KMSDataKeyForSearchAndExportPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "kms:EncryptionContextKeys" : [
            "aws:backup-search:search-job"
          ]
        },
        "StringLike" : {
          "kms:ViaService" : [
            "backup.*.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSBackupServiceLinkedRolePolicyForBackup

説明: AWS サービス間でユーザーに代わってバックアップを作成する AWS Backup アクセス許可を付与します

AWSBackupServiceLinkedRolePolicyForBackup は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 6 月 2 日 23:08 UTC
- 編集日時: 2025 年 11 月 10 日 19:19 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSBackupServiceLinkedRolePolicyForBackup

ポリシーのバージョン

ポリシーのバージョン: v21 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
      "Sid" : "EFSResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:Backup",
        "elasticfilesystem:DescribeTags"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/aws:elasticfilesystem:default-backup" : "enabled"
        }
      }
    },
    {
      "Sid" : "DescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources",
        "elasticfilesystem:DescribeFileSystems",
        "dynamodb:ListTables",
        "storagegateway:ListVolumes",
        "ec2:DescribeVolumes",
        "ec2:DescribeInstances",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "fsx:DescribeFileSystems",
        "fsx:DescribeVolumes",
        "s3:ListAllMyBuckets",
        "s3:GetBucketTagging"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SnapshotCopyTagPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CopySnapshot"
        }
      }
    },
    {
```

```
      "Sid" : "EC2CreateBackupTagPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*::snapshot/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AWSBackupManagedResource"
          ]
        }
      }
    },
    {
      "Sid" : "EC2CreateTagsPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*::snapshot/*"
      ],
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSBackupManagedResource" : "false"
        }
      }
    },
    {
      "Sid" : "EC2RDSDescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSnapshots",
        "ec2:DescribeSnapshotTierStatus",
        "ec2:DescribeImages",
        "rds:DescribeDBSnapshots",
        "rds:DescribeDBClusterSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EBSCopyPermissions",
      "Effect" : "Allow",
```

```
      "Action" : "ec2:CopySnapshot",
      "Resource" : "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Sid" : "EC2CopyPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:CopyImage",
      "Resource" : "*"
    },
    {
      "Sid" : "EC2ModifyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeregisterImage",
        "ec2:DeleteSnapshot",
        "ec2:ModifySnapshotTier"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSBackupManagedResource" : "false"
        }
      }
    },
    {
      "Sid" : "RDSInstanceAndSnashotPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:AddTagsToResource",
        "rds:CopyDBSnapshot",
        "rds:DeleteDBSnapshot",
        "rds:DeleteDBInstanceAutomatedBackup"
      ],
      "Resource" : "arn:aws:rds:*:*:snapshot:awsbackup:*"
    },
    {
      "Sid" : "RDSClusterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:AddTagsToResource",
        "rds:CopyDBClusterSnapshot",
        "rds:DeleteDBClusterSnapshot"
      ],
      "Resource" : "arn:aws:rds:*:*:cluster-snapshot:awsbackup:*"
```

```
    },
    {
      "Sid" : "RDSSnapshotTenantDatabasePermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:AddTagsToResource"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:snapshot-tenant-database:awsbackup:*"
      ]
    },
    {
      "Sid" : "KMSDescribePermissions",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "*"
    },
    {
      "Sid" : "KMSGrantPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListGrants",
        "kms:ReEncryptFrom",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com",
            "rds.*.amazonaws.com",
            "fsx.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "KMSCreateGrantPermissions",
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
```

```
        },
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com",
            "rds.*.amazonaws.com",
            "fsx.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "FsxPermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:CopyBackup",
        "fsx:TagResource",
        "fsx:DescribeBackups",
        "fsx:DeleteBackup"
      ],
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    },
    {
      "Sid" : "DynamoDBDeletePermissions",
      "Effect" : "Allow",
      "Action" : "dynamodb:DeleteBackup",
      "Resource" : "arn:aws:dynamodb:*:*:table/*/backup/*"
    },
    {
      "Sid" : "BackupGateway",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:ListVirtualMachines"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListTagsForBackupGateway",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:ListTagsForResource"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:vm/*"
    },
    {
```

```
      "Sid" : "DynamoDBPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListTagsOfResource",
        "dynamodb:DescribeTable"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*"
    },
    {
      "Sid" : "StorageGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:DescribeCachediSCSIVolumes",
        "storagegateway:DescribeStorediSCSIVolumes"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*/volume/*"
    },
    {
      "Sid" : "EventBridgePermissions",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:PutTargets",
        "events:DescribeRule",
        "events:EnableRule",
        "events:PutRule",
        "events:RemoveTargets",
        "events:ListTargetsByRule",
        "events:DisableRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/AwsBackupManagedRule*"
      ]
    },
    {
      "Sid" : "EventBridgeRulesPermissions",
      "Effect" : "Allow",
      "Action" : "events:ListRules",
      "Resource" : "*"
    },
    {
      "Sid" : "SSMSAPPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ssm-sap:GetOperation",
        "ssm-sap:UpdateHANABackupSettings"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TimestreamResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:ListDatabases",
        "timestream:ListTables",
        "timestream:ListTagsForResource",
        "timestream:DescribeDatabase",
        "timestream:DescribeTable",
        "timestream:GetAwsBackupStatus",
        "timestream:GetAwsRestoreStatus"
      ],
      "Resource" : [
        "arn:aws:timestream:*:*:database/*"
      ]
    },
    {
      "Sid" : "TimestreamPermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:DescribeEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftDescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeTags"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:snapshot:*/*",
        "arn:aws:redshift:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "RedshiftClusterSnapshotPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "redshift:DeleteClusterSnapshot"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:snapshot:*/*"
      ]
    },
    {
      "Sid" : "RedshiftClusterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "RedshiftServerlessGetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetSnapshot",
        "redshift-serverless:GetWorkgroup"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*",
        "arn:aws:redshift-serverless:*:*:workgroup/*",
        "arn:aws:redshift-serverless:*:*:snapshot/*"
      ]
    },
    {
      "Sid" : "RedshiftServerlessDeleteSnapshotPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:DeleteSnapshot"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:snapshot/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        }
```

```
      }
    },
    {
      "Sid" : "RedshiftServerlessListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListSnapshots",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:ListWorkgroups"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CloudformationStackPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStacks"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/*"
      ]
    },
    {
      "Sid" : "RecoveryPointTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:TagResource"
      ],
      "Resource" : "arn:aws:backup:*:*:recovery-point:*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    },
    {
      "Sid" : "DSQLListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dsql:ListClusters",
        "dsql:ListTagsForResource"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrgsListDelegatedAdmins",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "EKSClusterConfigurationBackup",
      "Effect" : "Allow",
      "Action" : [
        "eks:ListClusters",
        "eks:ListTagsForResource",
        "eks:DescribeCluster",
        "eks:ListAddons",
        "eks:DescribeAddon",
        "eks:ListNodegroups",
        "eks:DescribeNodegroup",
        "eks:ListPodIdentityAssociations",
        "eks:DescribePodIdentityAssociation",
        "eks:ListAccessEntries",
        "eks:DescribeAccessEntry",
        "eks:ListAssociatedAccessPolicies",
        "eks:ListFargateProfiles",
        "eks:DescribeFargateProfile",
        "ec2:DescribeLaunchTemplateVersions"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSBackupServiceLinkedRolePolicyForBackupTest

説明: AWS サービス間でユーザーに代わってバックアップを作成する AWS Backup アクセス許可を付与します

`AWSBackupServiceLinkedRolePolicyForBackupTest` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 5 月 12 日 17:37 UTC
- 編集日時: 2020 年 5 月 12 日 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBackupServiceLinkedRolePolicyForBackupTest`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
```

```
  "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"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSBackupServiceRolePolicyForBackup

説明: AWS サービス間でユーザーに代わってバックアップを作成する AWS Backup アクセス許可を付与します

AWSBackupServiceRolePolicyForBackup は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSBackupServiceRolePolicyForBackup をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2019 年 1 月 10 日 21:01 UTC
- 編集日時: 2025 年 11 月 10 日 19:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBackupServiceRolePolicyForBackup`

ポリシーのバージョン

ポリシーのバージョン: v23 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DynamoDBPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeTable",
        "dynamodb:CreateBackup"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*"
    },
    {
      "Sid" : "DynamoDBBackupResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeBackup",
        "dynamodb:DeleteBackup"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*/backup/*"
    },
    {
```

```
      "Sid" : "DynamoDBBackupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:AddTagsToResource",
        "rds:ListTagsForResource",
        "rds:DescribeDBSnapshots",
        "rds:CreateDBSnapshot",
        "rds:CopyDBSnapshot",
        "rds:DescribeDBInstances",
        "rds:CreateDBClusterSnapshot",
        "rds:DescribeDBClusters",
        "rds:DescribeDBClusterSnapshots",
        "rds:CopyDBClusterSnapshot",
        "rds:DescribeDBClusterAutomatedBackups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RDSInstanceAutomatedBackupPermissions",
      "Effect" : "Allow",
      "Action" : "rds:DeleteDBInstanceAutomatedBackup",
      "Resource" : "arn:aws:rds:*:*:auto-backup:*"
    },
    {
      "Sid" : "RDSClusterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:ModifyDBCluster"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "RDSClusterBackupPermissions",
      "Effect" : "Allow",
      "Action" : "rds:DeleteDBClusterAutomatedBackup",
      "Resource" : "arn:aws:rds:*:*:cluster-auto-backup:*"
    },
    {
      "Sid" : "RDSModifyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:ModifyDBInstance"
```

```
      ],
      "Resource" : [
        "arn:aws:rds:*:*:db:*"
      ]
    },
    {
      "Sid" : "RDSBackupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:DeleteDBSnapshot",
        "rds:ModifyDBSnapshotAttribute"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:snapshot:awsbackup:*"
      ]
    },
    {
      "Sid" : "RDSClusterModifyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:DeleteDBClusterSnapshot",
        "rds:ModifyDBClusterSnapshotAttribute"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:cluster-snapshot:awsbackup:*"
      ]
    },
    {
      "Sid" : "StorageGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:CreateSnapshot",
        "storagegateway:ListTagsForResource"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*/volume/*"
    },
    {
      "Sid" : "EBSCopyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopySnapshot"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*"
    },
```

```
    {
      "Sid" : "EC2CopyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopyImage"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EBSTagAndDeletePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Sid" : "EC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateImage",
        "ec2:DeregisterImage",
        "ec2:DescribeSnapshots",
        "ec2:DescribeTags",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceCreditSpecifications",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeElasticGpus",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSnapshotTierStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2TagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:image/*"
    },
```

```
    {
      "Sid" : "EC2ModifyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotAttribute",
        "ec2:ModifyImageAttribute"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        }
      }
    },
    {
      "Sid" : "EBSSnapshotTierPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotTier"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        }
      }
    },
    {
      "Sid" : "BackupVaultPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:DescribeBackupVault",
        "backup:CopyIntoBackupVault"
      ],
      "Resource" : "arn:aws:backup:*:*:backup-vault:*"
    },
    {
      "Sid" : "BackupVaultCopyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:CopyFromBackupVault"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "EFSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:Backup",
        "elasticfilesystem:DescribeTags"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*"
    },
    {
      "Sid" : "EBSResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot",
        "ec2:DeleteSnapshot",
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSDynamoDBPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "dynamodb.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "KMSPermissions",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "*"
    },
    {
      "Sid" : "KMSCreateGrantPermissions",
```

```
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        }
      }
    },
    {
      "Sid" : "KMSEC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:ebs:id"
        }
      }
    },
    {
      "Sid" : "GetResourcesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CancelCommand",
        "ssm:GetCommandInvocation"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "SSMSendPermissions",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSEC2-CreateVssSnapshot",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Sid" : "FsxBackupPermissions",
      "Effect" : "Allow",
      "Action" : "fsx:DescribeBackups",
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    },
    {
      "Sid" : "FsxCreateBackupPermissions",
      "Effect" : "Allow",
      "Action" : "fsx:CreateBackup",
      "Resource" : [
        "arn:aws:fsx:*:*:file-system/*",
        "arn:aws:fsx:*:*:backup/*",
        "arn:aws:fsx:*:*:volume/*"
      ]
    },
    {
      "Sid" : "FsxPermissions",
      "Effect" : "Allow",
      "Action" : "fsx:DescribeFileSystems",
      "Resource" : "arn:aws:fsx:*:*:file-system/*"
    },
    {
      "Sid" : "FsxVolumePermissions",
      "Effect" : "Allow",
      "Action" : "fsx:DescribeVolumes",
      "Resource" : "arn:aws:fsx:*:*:volume/*"
    },
    {
      "Sid" : "FsxListTagsPermissions",
      "Effect" : "Allow",
      "Action" : "fsx:ListTagsForResource",
      "Resource" : [
```

```
        "arn:aws:fsx:*:*:file-system/*",
        "arn:aws:fsx:*:*:volume/*"
      ]
    },
    {
      "Sid" : "FsxDeletePermissions",
      "Effect" : "Allow",
      "Action" : "fsx:DeleteBackup",
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    },
    {
      "Sid" : "FsxResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:ListTagsForResource",
        "fsx:ManageBackupPrincipalAssociations",
        "fsx:CopyBackup",
        "fsx:TagResource"
      ],
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    },
    {
      "Sid" : "DynamodbBackupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:StartAwsBackupJob",
        "dynamodb:ListTagsOfResource"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*"
    },
    {
      "Sid" : "BackupGatewayBackupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:Backup",
        "backup-gateway:ListTagsForResource"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:vm/*"
    },
    {
      "Sid" : "CloudformationStackPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStacks",
```

```
        "cloudformation:GetTemplate",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/*/*"
    },
    {
      "Sid" : "RedshiftCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:CreateClusterSnapshot",
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeTags"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:snapshot:*/*",
        "arn:aws:redshift:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "RedshiftSnapshotPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DeleteClusterSnapshot"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:snapshot:*/*"
      ]
    },
    {
      "Sid" : "RedshiftPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "RedshiftResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:CreateTags"
```

```
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:snapshot:*/*"
      ]
    },
    {
      "Sid" : "RedshiftServerlessCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:CreateSnapshot"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:snapshot/*",
        "arn:aws:redshift-serverless:*:*:namespace/*"
      ]
    },
    {
      "Sid" : "RedshiftServerlessSnapshotPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:DeleteSnapshot"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:snapshot/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        }
      }
    },
    {
      "Sid" : "RedshiftServerlessGetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetNamespace"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*"
      ]
    },
    {
      "Sid" : "RedshiftServerlessResourcePermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "redshift-serverless:GetSnapshot",
        "redshift-serverless:TagResource"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:snapshot/*"
      ]
    },
    {
      "Sid" : "RedshiftServerlessListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListSnapshots",
        "redshift-serverless:ListTagsForResource"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "TimestreamResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:StartAwsBackupJob",
        "timestream:GetAwsBackupStatus",
        "timestream:ListTables",
        "timestream:ListDatabases",
        "timestream:ListTagsForResource",
        "timestream:DescribeTable",
        "timestream:DescribeDatabase"
      ],
      "Resource" : [
        "arn:aws:timestream:*:*:database/*"
      ]
    },
    {
      "Sid" : "TimestreamEndpointPermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:DescribeEndpoints"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "SSMSAPPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:GetOperation",
        "ssm-sap:ListDatabases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMSAPResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:BackupDatabase",
        "ssm-sap:UpdateHanaBackupSettings",
        "ssm-sap:GetDatabase",
        "ssm-sap:ListTagsForResource"
      ],
      "Resource" : "arn:aws:ssm-sap:*:*:*"
    },
    {
      "Sid" : "RecoveryPointTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:TagResource"
      ],
      "Resource" : "arn:aws:backup:*:*:recovery-point:*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    },
    {
      "Sid" : "DSQLResourcePermissionsForBackup",
      "Effect" : "Allow",
      "Action" : [
        "dsql:StartBackupJob",
        "dsql:GetBackupJob",
        "dsql:StopBackupJob",
        "dsql:GetCluster",
        "dsql:ListClusters",
        "dsql:ListTagsForResource"
      ],
```

```
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "KMSDSQLPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "dsql.*.amazonaws.com"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:dsql:ClusterId"
        }
      }
    },
    {
      "Sid" : "EKSClusterConfigurationBackup",
      "Effect" : "Allow",
      "Action" : [
        "eks:ListClusters",
        "eks:ListTagsForResource",
        "eks:DescribeCluster",
        "eks:ListAddons",
        "eks:DescribeAddon",
        "eks:ListNodegroups",
        "eks:DescribeNodegroup",
        "eks:ListPodIdentityAssociations",
        "eks:DescribePodIdentityAssociation",
        "eks:ListAccessEntries",
        "eks:DescribeAccessEntry",
        "eks:ListAssociatedAccessPolicies",
        "eks:ListFargateProfiles",
        "eks:DescribeFargateProfile",
        "ec2:DescribeLaunchTemplateVersions"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "CreateBackupAccessEntry",
      "Effect" : "Allow",
      "Action" : [
        "eks:CreateAccessEntry"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/*"
    },
    {
      "Sid" : "AssociateBackupAccessPolicy",
      "Effect" : "Allow",
      "Action" : [
        "eks:AssociateAccessPolicy",
        "eks:DisassociateAccessPolicy"
      ],
      "Resource" : "arn:aws:eks:*:*:access-entry/*",
      "Condition" : {
        "StringEquals" : {
          "eks:policyArn" : "arn:aws:eks::aws:cluster-access-policy/
AWSBackupFullAccessPolicyForBackup",
          "eks:accessScope" : "cluster"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSBackupServiceRolePolicyForIndexing

説明: AWS Backup が復旧ポイントのインデックスを作成するために必要なアクセス許可を含むポリシー。

AWSBackupServiceRolePolicyForIndexing は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSBackupServiceRolePolicyForIndexing をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 12 月 17 日 18:37 UTC
- 編集日時: 2024 年 12 月 17 日 18:37 UTC
- ARN: arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForIndexing

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EBSReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
```

```
    {
      "Sid" : "EBSDirectReadAPIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ebs:ListSnapshotBlocks",
        "ebs:GetSnapshotBlock"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Sid" : "KMSDataKeyForEC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSBackupServiceRolePolicyForItemRestores

説明: AWS Backup が復旧ポイント内の個々の項目を復元するために必要なアクセス許可を含むポリシー

`AWSBackupServiceRolePolicyForItemRestores` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSBackupServiceRolePolicyForItemRestores をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 12 月 17 日 18:37 UTC
- 編集日時: 2024 年 12 月 17 日 18:37 UTC
- ARN: arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForItemRestores

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EBSReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
```

```
      "Sid" : "EBSDirectReadAPIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ebs:ListSnapshotBlocks",
        "ebs:GetSnapshotBlock"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Sid" : "S3ReadonlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3PermissionsForFileLevelRestore",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:AbortMultipartUpload",
        "s3:ListMultipartUploadParts"
      ],
      "Resource" : "arn:aws:s3:::*/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "KMSDataKeyForS3AndEC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
```

```
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com",
            "s3.*.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSBackupServiceRolePolicyForRestores

説明: AWS サービス間でユーザーに代わって復元を実行する AWS Backup アクセス許可を提供します。このポリシーには、復元プロセスの一部である EBS ボリューム、RDS インスタンス、EFS ファイルシステムなどの AWS リソースを作成および削除するアクセス許可が含まれています。

`AWSBackupServiceRolePolicyForRestores` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSBackupServiceRolePolicyForRestores` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2019 年 1 月 12 日 00:23 UTC
- 編集日時: 2025 年 11 月 10 日 19:34 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v25 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DynamoDBPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:Scan",
        "dynamodb:Query",
        "dynamodb:UpdateItem",
        "dynamodb:PutItem",
        "dynamodb:GetItem",
        "dynamodb:DeleteItem",
        "dynamodb:BatchWriteItem",
        "dynamodb:DescribeTable"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*"
    },
    {
      "Sid" : "DynamoDBBackupResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:RestoreTableFromBackup"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*/backup/*"
    },
    {
      "Sid" : "EBSPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateVolume",
        "ec2:DeleteVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "Sid" : "EC2DescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSnapshotTierStatus",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateTagsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:route-table/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonFSx" : "ManagedByAmazonFSx"
        }
      }
    },
    {
      "Sid" : "StorageGatewayVolumePermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:DeleteVolume",
        "storagegateway:DescribeCachediSCSIVolumes",
        "storagegateway:DescribeStorediSCSIVolumes",
        "storagegateway:AddTagsToResource"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*/volume/*"
    },
    {
      "Sid" : "StorageGatewayGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:DescribeGatewayInformation",
        "storagegateway:CreateStorediSCSIVolume",
        "storagegateway:CreateCachediSCSIVolume"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*"
    },
    {
      "Sid" : "StorageGatewayListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:ListVolumes"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:*"
    },
    {
      "Sid" : "RDSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBInstances",
        "rds:DescribeDBSnapshots",
        "rds:ListTagsForResource",
        "rds:RestoreDBInstanceFromDBSnapshot",
        "rds:DeleteDBInstance",
        "rds:AddTagsToResource",
        "rds:DescribeDBClusters",
        "rds:RestoreDBClusterFromSnapshot",
        "rds:DeleteDBCluster",
        "rds:RestoreDBInstanceToPointInTime",
        "rds:DescribeDBClusterSnapshots",
        "rds:RestoreDBClusterToPointInTime",
        "rds:CreateTenantDatabase",
```

```
        "rds:DeleteTenantDatabase"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EFSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:Restore",
        "elasticfilesystem:CreateFilesystem",
        "elasticfilesystem:DescribeFilesystems",
        "elasticfilesystem:DeleteFilesystem",
        "elasticfilesystem:TagResource"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*"
    },
    {
      "Sid" : "KMSDescribePermissions",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "*"
    },
    {
      "Sid" : "DSQLResourcePermissionsForRestore",
      "Effect" : "Allow",
      "Action" : [
        "dsql:StartRestoreJob",
        "dsql:GetRestoreJob",
        "dsql:StopRestoreJob",
        "dsql:TagResource",
        "dsql:CreateCluster",
        "dsql:PutMultiRegionProperties",
        "dsql:PutWitnessRegion",
        "dsql:UpdateCluster",
        "dsql:AddPeerCluster",
        "dsql:RemovePeerCluster",
        "dsql:GetCluster"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "KMSPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "dynamodb.*.amazonaws.com",
            "ec2.*.amazonaws.com",
            "elasticfilesystem.*.amazonaws.com",
            "rds.*.amazonaws.com",
            "redshift.*.amazonaws.com",
            "dsql.*.amazonaws.com",
            "redshift-serverless.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "KMSCreateGrantPermissions",
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        }
      }
    },
    {
      "Sid" : "EBSSnapshotBlockPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ebs:CompleteSnapshot",
        "ebs:StartSnapshot",
        "ebs:PutSnapshotBlock"
      ],
```

```
      "Resource" : "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Sid" : "RDSResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:CreateDBInstance"
      ],
      "Resource" : "arn:aws:rds:*:*:db:*"
    },
    {
      "Sid" : "EC2DeleteAndRestorePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot",
        "ec2:DeleteTags",
        "ec2:RestoreSnapshotTier"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        }
      }
    },
    {
      "Sid" : "EC2CreateTagsScopedPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws:backup:source-resource"
          ]
        }
      }
    },
    {
      "Sid" : "EC2RunInstancesPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2TerminateInstancesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Sid" : "EC2CreateTagsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:CreateAction" : [
            "RunInstances",
            "CreateVolume"
          ]
        }
      }
    },
    {
      "Sid" : "FsxPermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:CreateFileSystemFromBackup"
      ],
      "Resource" : [
        "arn:aws:fsx:*:*:file-system/*",
        "arn:aws:fsx:*:*:backup/*"
      ]
    },
    {
```

```
      "Sid" : "FsxTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeFileSystems",
        "fsx:TagResource"
      ],
      "Resource" : "arn:aws:fsx:*:*:file-system/*"
    },
    {
      "Sid" : "FsxBackupPermissions",
      "Effect" : "Allow",
      "Action" : "fsx:DescribeBackups",
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    },
    {
      "Sid" : "FsxDeletePermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DeleteFileSystem",
        "fsx:UntagResource"
      ],
      "Resource" : "arn:aws:fsx:*:*:file-system/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        }
      }
    },
    {
      "Sid" : "FsxDescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeVolumes"
      ],
      "Resource" : "arn:aws:fsx:*:*:volume/*"
    },
    {
      "Sid" : "FsxVolumeTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:CreateVolumeFromBackup",
        "fsx:TagResource"
      ],
      "Resource" : [
```

```
        "arn:aws:fsx:*:*:volume/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws:backup:source-resource"
          ]
        }
      }
    },
    {
      "Sid" : "FsxBackupTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:CreateVolumeFromBackup",
        "fsx:TagResource"
      ],
      "Resource" : [
        "arn:aws:fsx:*:*:storage-virtual-machine/*",
        "arn:aws:fsx:*:*:backup/*",
        "arn:aws:fsx:*:*:volume/*"
      ]
    },
    {
      "Sid" : "FsxVolumePermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DeleteVolume",
        "fsx:UntagResource"
      ],
      "Resource" : "arn:aws:fsx:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        }
      }
    },
    {
      "Sid" : "DSPermissions",
      "Effect" : "Allow",
      "Action" : "ds:DescribeDirectories",
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "DynamoDBRestorePermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:RestoreTableFromAwsBackup"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*"
    },
    {
      "Sid" : "GatewayRestorePermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:Restore"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:hypervisor/*"
    },
    {
      "Sid" : "CloudformationChangeSetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:TagResource"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:*/*/*"
    },
    {
      "Sid" : "RedshiftClusterSnapshotPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:RestoreFromClusterSnapshot",
        "redshift:RestoreTableFromClusterSnapshot"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:snapshot:*/*",
        "arn:aws:redshift:*:*:cluster:*",
        "arn:aws:redshift-serverless:*:*:snapshot/*"
      ]
    },
    {
      "Sid" : "RedshiftClusterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters"
      ],
```

```
      "Resource" : [
        "arn:aws:redshift:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "RedshiftTablePermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeTableRestoreStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftServerlessSnapshotPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:RestoreTableFromSnapshot"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*",
        "arn:aws:redshift-serverless:*:*:workgroup/*",
        "arn:aws:redshift-serverless:*:*:snapshot/*"
      ]
    },
    {
      "Sid" : "RedshiftServerlessNamespacePermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetNamespace"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*"
      ]
    },
    {
      "Sid" : "RedshiftServerlessTablePermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetTableRestoreStatus"
      ],
      "Resource" : [
        "*"
      ]
    },
```

```
    {
      "Sid" : "TimestreamResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:StartAwsRestoreJob",
        "timestream:GetAwsRestoreStatus",
        "timestream:ListTables",
        "timestream:ListTagsForResource",
        "timestream:ListDatabases",
        "timestream:DescribeTable",
        "timestream:DescribeDatabase"
      ],
      "Resource" : [
        "arn:aws:timestream:*:*:database/*"
      ]
    },
    {
      "Sid" : "TimestreamEndpointPermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:DescribeEndpoints"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EKSClusterRestore",
      "Effect" : "Allow",
      "Action" : [
        "eks:CreateCluster",
        "eks:DescribeCluster",
        "eks:CreateAccessEntry",
        "eks:DescribeAccessEntry",
        "eks:AssociateAccessPolicy",
        "eks:ListAssociatedAccessPolicies",
        "eks:CreateAddon",
        "eks:DescribeAddon",
        "eks:CreateNodegroup",
        "eks:DescribeNodegroup",
        "eks:CreateFargateProfile",
        "eks:DescribeFargateProfile",
        "eks:CreatePodIdentityAssociation",
        "eks:DescribePodIdentityAssociation",
```

```
        "eks:TagResource"
      ],
      "Resource" : [
        "arn:aws:eks:*:*:access-entry/*",
        "arn:aws:eks:*:*:addon/*",
        "arn:aws:eks:*:*:cluster/*",
        "arn:aws:eks:*:*:fargateprofile/*",
        "arn:aws:eks:*:*:nodegroup/*",
        "arn:aws:eks:*:*:podidentityassociation/*"
      ]
    },
    {
      "Sid" : "AssociateRestoreAccessPolicy",
      "Effect" : "Allow",
      "Action" : [
        "eks:AssociateAccessPolicy",
        "eks:DisassociateAccessPolicy"
      ],
      "Resource" : "arn:aws:eks:*:*:access-entry/*",
      "Condition" : {
        "StringEquals" : {
          "eks:policyArn" : "arn:aws:eks::aws:cluster-access-policy/
AWSBackupFullAccessPolicyForRestore",
          "eks:accessScope" : "cluster"
        }
      }
    },
    {
      "Sid" : "CreateClusterIAMPerms",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "eks.amazonaws.com",
            "ec2.amazonaws.com",
            "pods.eks.amazonaws.com",
            "backup.amazonaws.com"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "CreateEKSNodeGroupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeSubnets",
        "ec2:RunInstances",
        "iam:GetRole",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EKSNodeGroupTagOnCreate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances"
          ]
        }
      }
    },
    {
      "Sid" : "BackupRestoreJobManagementPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:StartRestoreJob",
        "backup:ListRestoreJobs",
        "backup:ListRecoveryPointsByBackupVault",
        "backup:DescribeRestoreJob"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSBackupServiceRolePolicyForS3Backup

説明: AWS Backup が任意の S3 バケット内のデータをバックアップするために必要なアクセス許可を含むポリシー。これには、すべての S3 オブジェクトへの読み取りアクセスと、すべての KMS キーに対する復号化アクセスが含まれます。

`AWSBackupServiceRolePolicyForS3Backup` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSBackupServiceRolePolicyForS3Backup` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 2 月 18 日 17:40 UTC
- 編集日時: 2024 年 5 月 17 日 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForS3Backup`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSBackupServiceRolePolicyForS3Restore

説明: AWS Backup が S3 バックアップをバケットに復元するために必要なアクセス許可を含むポリシー。これには、すべての S3 バケットへの読み取り/書き込み権限、およびすべての KMS キーの GenerateDataKey と DescribeKey の生成権限が含まれます。

`AWSBackupServiceRolePolicyForS3Restore` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSBackupServiceRolePolicyForS3Restore` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 2 月 18 日 17:39 UTC
- 編集日時: 2023 年 2 月 7 日 00:06 UTC

- ARN: arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForS3Restore

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSBackupServiceRolePolicyForScans

説明: AWS Backup リカバリポイントでマルウェアスキャンを実行するための AWS Backup アクセス許可を付与します

AWSBackupServiceRolePolicyForScans は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSBackupServiceRolePolicyForScans をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 11 月 20 日 03:34 UTC
- 編集日時: 2025 年 11 月 20 日 03:34 UTC
- ARN: arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForScans

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GuardDutyMalwareScanPermissions",
      "Effect" : "Allow",
      "Action" : [
        "guardduty:StartMalwareScan",
        "guardduty:GetMalwareScan"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMPassPermissions",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "iam:PassedToService" : "malware-protection.guardduty.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EC2ReadAPIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSBatchFullAccess

説明: Batch AWS リソースへのフルアクセスを提供します。

AWSBatchFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSBatchFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2016 年 12 月 6 日 19:35 UTC
- 編集日時: 2022 年 10 月 24 日 16:09 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSBatchServiceEventTargetRole

説明: AWS バッチジョブ送信の CloudWatch イベントターゲットを有効にするポリシー

AWSBatchServiceEventTargetRole は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSBatchServiceEventTargetRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2018 年 2 月 28 日 22:31 UTC
- 編集日時: 2018 年 2 月 28 日 22:31 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSBatchServiceEventTargetRole

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSBatchServiceRole

説明: EC2、Autoscaling、EC2 Container Service、Cloudwatch Logs などの関連サービスへのアクセスを許可する AWS Batch サービスロールのポリシー。

AWSBatchServiceRole は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSBatchServiceRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2016 年 12 月 6 日 19:36 UTC
- 編集日時: 2023 年 12 月 5 日 18:49 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSBatchServiceRole

ポリシーのバージョン

ポリシーのバージョン: v13 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSBatchServiceRolePolicyForSageMaker

説明: AWS Batch が Amazon SageMaker ワークロードをキューイングおよび管理するためのアクセスを提供します

AWSBatchServiceRolePolicyForSageMaker は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2025 年 7 月 15 日 21:37 UTC
- 編集日時: 2025 年 7 月 15 日 21:37 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSBatchServiceRolePolicyForSageMaker

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
        "sagemaker:StopTrainingJob",
        "sagemaker:ListTags"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:training-job/AWSBatch*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateTrainingJob"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-plan/*",
        "arn:aws:sagemaker:*:*:reserved-capacity/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:training-job/AWSBatch*",
      "Condition" : {
        "StringEquals" : {
          "sagemaker:TaggingAction" : "CreateTrainingJob"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListTrainingJobs",
        "sagemaker:Search"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com"
          ]
```

```
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSBCMDataExportsServiceRolePolicy

説明: Billing and Cost Management Data Exports に、顧客に代わって Amazon S3 などのターゲットロケーションにデータをエクスポートするための AWS サービスデータへのアクセスを提供するサービスにリンクされたロール。

`AWSBCMDataExportsServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2024 年 6 月 10 日 17:40 UTC
- 編集日時: 2024 年 6 月 10 日 17:40 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBCMDataExportsServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CostOptimizationRecommendationAccess",
      "Effect" : "Allow",
      "Action" : [
        "cost-optimization-hub:ListEnrollmentStatuses",
        "cost-optimization-hub:ListRecommendations"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSBillingConductorFullAccess

説明: AWSBillingConductorFullAccess 管理ポリシーを使用して、 AWS Billing Conductor (ABC) コンソールと APIs への完全なアクセスを許可します。このポリシーにより、ユーザーは ABC リソースを一覧表示、作成、削除できます。

`AWSBillingConductorFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSBillingConductorFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 4 月 13 日 18:02 UTC
- 編集日時: 2025 年 11 月 27 日 01:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBillingConductorFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "billingconductor:*",
        "organizations:ListAccounts",
        "pricing:DescribeServices",
        "pricing:GetAttributeValues",
        "pricing:GetProducts",
        "organizations:ListRoots",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListChildren",
        "organizations:DescribeAccount",
        "organizations:DescribeResponsibilityTransfer",
        "organizations:ListInboundResponsibilityTransfers"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSBillingConductorReadOnlyAccess

説明: AWSBillingConductorReadOnlyAccess 管理ポリシーを使用して、 AWS Billing Conductor (ABC) コンソールと APIs への読み取り専用アクセスを許可します。このポリシーは、すべての ABC リソースを取得して一覧表示するアクセス許可を付与します。リソースを作成または削除したりする機能は含まれません。

`AWSBillingConductorReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSBillingConductorReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 4 月 13 日 18:02 UTC
- 編集日時: 2025 年 9 月 18 日 00:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBillingConductorReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "billingconductor:List*",
        "billingconductor:GetBillingGroupCostReport",
        "organizations:ListAccounts",
        "pricing:DescribeServices",
        "pricing:GetAttributeValues",
        "pricing:GetProducts",
        "organizations:ListRoots",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListChildren",
        "organizations:DescribeAccount"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSBillingReadOnlyAccess

説明: 請求コンソールでの請求の閲覧をユーザーに許可します。

AWSBillingReadOnlyAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSBillingReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 8 月 27 日 20:08 UTC
- 編集日時: 2025 年 11 月 18 日 21:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBillingReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v14 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
        "aws-portal:ViewBilling",
        "billing:GetBillingData",
        "billing:GetBillingDetails",
        "billing:GetBillingNotifications",
        "billing:GetBillingPreferences",
        "billing:GetCredits",
        "billing:GetContractInformation",
        "billing:GetIAMAccessPreference",
        "billing:GetSellerOfRecord",
        "billing:ListBillingViews",
        "budgets:ViewBudget",
        "budgets:DescribeBudgetActionsForBudget",
        "budgets:DescribeBudgetAction",
        "budgets:DescribeBudgetActionsForAccount",
        "budgets:DescribeBudgetActionHistories",
```

```
        "ce:DescribeCostCategoryDefinition",
        "ce:GetCostAndUsage",
        "ce:ListCostCategoryDefinitions",
        "ce:ListTagsForResource",
        "ce:ListCostAllocationTags",
        "ce:ListCostAllocationTagBackfillHistory",
        "ce:GetTags",
        "ce:GetDimensionValues",
        "ce:GetCostAndUsageComparisons",
        "ce:GetCostComparisonDrivers",
        "consolidatedbilling:ListLinkedAccounts",
        "consolidatedbilling:GetAccountBillingRole",
        "cur:GetClassicReport",
        "cur:GetClassicReportPreferences",
        "cur:GetUsageReport",
        "cur:DescribeReportDefinitions",
        "freetier:GetFreeTierAlertPreference",
        "freetier:GetFreeTierUsage",
        "freetier:GetAccountPlanState",
        "freetier:GetAccountActivity",
        "freetier:ListAccountActivities",
        "invoicing:BatchGetInvoiceProfile",
        "invoicing:GetInvoiceEmailDeliveryPreferences",
        "invoicing:GetInvoicePDF",
        "invoicing:GetInvoiceUnit",
        "invoicing:GetInvoiceCorrection",
        "invoicing:ListInvoiceSummaries",
        "invoicing:ListInvoiceUnits",
        "invoicing:GetProcurementPortalPreference",
        "invoicing:ListProcurementPortalPreferences",
        "invoicing:ListTagsForResource",
        "invoicing:ListInvoiceCorrections",
        "mapcredits:ListQuarterSpend",
        "mapcredits:ListAssociatedPrograms",
        "mapcredits:ListQuarterCredits",
        "payments:GetFinancingApplication",
        "payments:GetFinancingLine",
        "payments:GetFinancingLineWithdrawal",
        "payments:GetFinancingOption",
        "payments:GetPaymentInstrument",
        "payments:GetPaymentStatus",
        "payments:ListFinancingApplications",
        "payments:ListFinancingLines",
        "payments:ListFinancingLineWithdrawals",
```

```
        "payments:ListPaymentInstruments",
        "payments:ListPaymentPreferences",
        "payments:ListPaymentProgramOptions",
        "payments:ListPaymentProgramStatus",
        "payments:ListTagsForResource",
        "purchase-orders:GetPurchaseOrder",
        "purchase-orders:ViewPurchaseOrders",
        "purchase-orders:ListPurchaseOrderInvoices",
        "purchase-orders:ListPurchaseOrders",
        "purchase-orders:ListTagsForResource",
        "sustainability:GetCarbonFootprintSummary",
        "tax:GetTaxRegistrationDocument",
        "tax:GetTaxInheritance",
        "tax:ListTaxRegistrations"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSBillingServiceRolePolicy

説明: 請求サービスが、派生した請求ビューの請求ビューデータへのアクセスを検証できるようにします

`AWSBillingServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2025 年 9 月 11 日 16:19 UTC
- 編集日時: 2025 年 9 月 11 日 16:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBillingServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM

説明: このポリシーは、 AWS リソースを制御するアクセス許可を付与します。例えば、 AWS Systems Manager (SSM) スクリプトを実行して EC2 または RDS インスタンスを起動および停止します。

AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 5 月 25 日 19:03 UTC
- 編集日時: 2022 年 5 月 25 日 19:03 UTC
- ARN: arn:aws:iam::aws:policy/AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSBudgetsActionsWithAWSResourceControlAccess

説明: AWS Budgets Actions を使用して 経由で実行中の AWS リソースの状態を制御するなど、Budgets Actions へのフルアクセスを提供します AWS マネジメントコンソール

`AWSBudgetsActionsWithAWSResourceControlAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSBudgetsActionsWithAWSResourceControlAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 10 月 15 日 17:19 UTC
- 編集日時: 2020 年 10 月 15 日 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBudgetsActionsWithAWSResourceControlAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSBudgetsReadOnlyAccess

説明: 経由で AWS Budgets コンソールへの読み取り専用アクセスを提供します AWS マネジメントコンソール。

`AWSBudgetsReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSBudgetsReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 10 月 15 日 17:18 UTC
- 編集日時: 2024 年 6 月 17 日 17:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBudgetsReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSBudgetsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-portal:ViewBilling",
        "budgets:ViewBudget",
        "budgets:Describe*",
        "budgets:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSBugBustFullAccess

説明: この IAM ポリシーは、 AWS BugBust コンソールへのフルアクセスをユーザーに付与します

`AWSBugBustFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSBugBustFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 6 月 24 日 07:03 UTC
- 編集日時: 2021 年 7 月 22 日 20:04 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSBugBustPlayerAccess

説明: この IAM ポリシーは、in AWS BugBust イベントに参加するためのアクセス権をユーザーに付与します

AWSBugBustPlayerAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSBugBustPlayerAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 6 月 24 日 07:15 UTC
- 編集日時: 2021 年 6 月 24 日 07:15 UTC
- ARN: arn:aws:iam::aws:policy/AWSBugBustPlayerAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSBugBustServiceRolePolicy

説明: ユーザーに代わってリソースにアクセスするためのアクセス許可を AWS BugBust に付与します

AWSBugBustServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 6 月 24 日 06:59 UTC
- 編集日時: 2021 年 6 月 24 日 06:59 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSBugBustServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codeguru-reviewer:ListRecommendations",
        "codeguru-reviewer:UntagResource",
        "codeguru-reviewer:DescribeCodeReview"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/bugbust" : "enabled"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSCertificateManagerFullAccess

説明: AWS Certificate Manager (ACM) へのフルアクセスを提供します

AWSCertificateManagerFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCertificateManagerFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2016 年 1 月 21 日 17:02 UTC
- 編集日時: 2020 年 8 月 17 日 22:18 UTC
- ARN: arn:aws:iam::aws:policy/AWSCertificateManagerFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSCertificateManagerPrivateCAAuditor

説明: AWS Certificate Manager Private Certificate Authority への監査アクセスを提供します

`AWSCertificateManagerPrivateCAAuditor` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSCertificateManagerPrivateCAAuditor` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 10 月 23 日 16:51 UTC

- 編集日時: 2020 年 8 月 17 日 22:54 UTC
- ARN: arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAAuditor

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSCertificateManagerPrivateCAFullAccess

説明: AWS Certificate Manager プライベート認証機関へのフルアクセスを提供します

`AWSCertificateManagerPrivateCAFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSCertificateManagerPrivateCAFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 10 月 23 日 16:54 UTC
- 編集日時: 2018 年 10 月 23 日 16:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSCertificateManagerPrivateCAPrivilegedUser

説明: Certificate Manager Private Certificate Authority への特権 AWS 証明書ユーザーアクセスを提供します

`AWSCertificateManagerPrivateCAPrivilegedUser` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSCertificateManagerPrivateCAPrivilegedUser` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 6 月 20 日 17:43 UTC
- 編集日時: 2025 年 1 月 22 日 19:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAPrivilegedUser`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "ArnLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:*:*:template/*CACertificate*/V*"
          ]
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "ArnNotLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:*:*:template/*CACertificate*/V*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "acm-pca:RevokeCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:ListPermissions"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:ListCertificateAuthorities"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSCertificateManagerPrivateCAReadOnly

説明: AWS Certificate Manager プライベート認証機関への読み取り専用アクセスを提供します

`AWSCertificateManagerPrivateCAReadOnly` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSCertificateManagerPrivateCAReadOnly` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 10 月 23 日 16:57 UTC

- 編集日時: 2020 年 8 月 17 日 22:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAReadOnly`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSCertificateManagerPrivateCAUser

説明: Certificate Manager プライベート認証機関への AWS 証明書ユーザーアクセスを提供します

AWSCertificateManagerPrivateCAUser は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCertificateManagerPrivateCAUser をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 10 月 23 日 16:53 UTC
- 編集日時: 2025 年 1 月 22 日 15:52 UTC
- ARN: arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAUser

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "ArnLike" : {
```

```
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:*:*:template/EndEntityCertificate/V*"
          ]
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "ArnNotLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:*:*:template/EndEntityCertificate/V*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:RevokeCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:ListPermissions"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:ListCertificateAuthorities"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSCertificateManagerReadOnly

説明: AWS Certificate Manager (ACM) への読み取り専用アクセスを提供します。

`AWSCertificateManagerReadOnly` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSCertificateManagerReadOnly` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2016 年 1 月 21 日 17:07 UTC
- 編集日時: 2021 年 3 月 15 日 16:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerReadOnly`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "acm:DescribeCertificate",
      "acm:ListCertificates",
      "acm:GetCertificate",
```

```
      "acm:ListTagsForCertificate",
      "acm:GetAccountConfiguration"
    ],
    "Resource" : "*"
  }
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSChatbotServiceLinkedRolePolicy

説明: AWS Chatbot で使用されるサービスにリンクされたロール。

AWSChatbotServiceLinkedRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 11 月 18 日 16:39 UTC
- 編集日時: 2019 年 11 月 18 日 16:39 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSChatbotServiceLinkedRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSCleanRoomsFullAccess

説明: AWS Clean Rooms リソースへのフルアクセスと、関連する へのアクセスを許可します AWS のサービス。

AWSCleanRoomsFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCleanRoomsFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 1 月 12 日 16:10 UTC
- 編集日時: 2024 年 3 月 21 日 15:35 UTC
- ARN: arn:aws:iam::aws:policy/AWSCleanRoomsFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSCleanRoomsFullAccessNoQuerying

説明: コラボレーションでのクエリと関連 へのアクセスを除き、 AWS Clean Rooms リソースへのフルアクセスを許可します AWS のサービス。

`AWSCleanRoomsFullAccessNoQuerying` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSCleanRoomsFullAccessNoQuerying` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 1 月 12 日 16:12 UTC
- 編集日時: 2025 年 8 月 13 日 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsFullAccessNoQuerying`

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CleanRoomsAccess",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:BatchGetCollaborationAnalysisTemplate",
        "cleanrooms:BatchGetSchema",
        "cleanrooms:BatchGetSchemaAnalysisRule",
        "cleanrooms:CreateAnalysisTemplate",
        "cleanrooms:CreateCollaboration",
        "cleanrooms:CreateConfiguredTable",
        "cleanrooms:CreateConfiguredTableAnalysisRule",
        "cleanrooms:CreateConfiguredTableAssociation",
        "cleanrooms:CreateMembership",
        "cleanrooms:DeleteAnalysisTemplate",
        "cleanrooms:DeleteCollaboration",
        "cleanrooms:DeleteConfiguredTable",
        "cleanrooms:DeleteConfiguredTableAnalysisRule",
        "cleanrooms:DeleteConfiguredTableAssociation",
        "cleanrooms:DeleteMember",
        "cleanrooms:DeleteMembership",
        "cleanrooms:GetAnalysisTemplate",
        "cleanrooms:GetCollaborationAnalysisTemplate",
        "cleanrooms:GetCollaboration",
        "cleanrooms:GetConfiguredTable",
        "cleanrooms:GetConfiguredTableAnalysisRule",
        "cleanrooms:GetConfiguredTableAssociation",
        "cleanrooms:GetMembership",
        "cleanrooms:GetProtectedQuery",
        "cleanrooms:GetSchema",
        "cleanrooms:GetSchemaAnalysisRule",
        "cleanrooms:ListAnalysisTemplates",
        "cleanrooms:ListCollaborationAnalysisTemplates",
        "cleanrooms:ListCollaborations",
        "cleanrooms:ListConfiguredTableAssociations",
        "cleanrooms:ListConfiguredTables",
        "cleanrooms:ListMembers",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListProtectedQueries",
```

```
        "cleanrooms:ListSchemas",
        "cleanrooms:UpdateAnalysisTemplate",
        "cleanrooms:UpdateCollaboration",
        "cleanrooms:UpdateConfiguredTable",
        "cleanrooms:UpdateConfiguredTableReference",
        "cleanrooms:UpdateConfiguredTableAllowedColumns",
        "cleanrooms:UpdateConfiguredTableAnalysisRule",
        "cleanrooms:UpdateConfiguredTableAssociation",
        "cleanrooms:UpdateMembership",
        "cleanrooms:ListTagsForResource",
        "cleanrooms:UntagResource",
        "cleanrooms:TagResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CleanRoomsNoQuerying",
      "Effect" : "Deny",
      "Action" : [
        "cleanrooms:StartProtectedQuery",
        "cleanrooms:UpdateProtectedQuery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/*cleanrooms*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ListRolesToPickServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "GetRoleAndListRolePoliciesToInspectServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/*cleanrooms*"
    },
    {
      "Sid" : "ListPoliciesToInspectServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListPolicies"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetPolicyToInspectServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
      ],
      "Resource" : "arn:aws:iam::*:policy/*cleanrooms*"
    },
    {
      "Sid" : "ConsoleDisplayTables",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetSchema",
        "glue:GetSchemaVersion",
        "glue:BatchGetPartition"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "EstablishLogDeliveries",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SetupLogGroupsDescribe",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SetupLogGroupsCreate",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/cleanrooms*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
```

```
      "Sid" : "SetupLogGroupsResourcePolicy",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeResourcePolicies",
        "logs:PutResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ConsoleLogSummaryQueryLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:StartQuery"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/cleanrooms*"
    },
    {
      "Sid" : "ConsoleLogSummaryObtainLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:GetQueryResults"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSCleanRoomsMLFullAccess

説明: AWS Clean Rooms ML リソースへのフルアクセスと、関連する へのアクセスを許可します AWS のサービス。

AWSCleanRoomsMLFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCleanRoomsMLFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 11 月 29 日 21:02 UTC
- 編集日時: 2025 年 1 月 10 日 20:07 UTC
- ARN: arn:aws:iam::aws:policy/AWSCleanRoomsMLFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
      "Sid" : "PassServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/cleanrooms-ml*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "cleanrooms-ml.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CleanRoomsConsoleNavigation",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:GetCollaboration",
        "cleanrooms:BatchGetSchema",
        "cleanrooms:GetConfiguredAudienceModelAssociation",
        "cleanrooms:GetMembership",
        "cleanrooms:ListAnalysisTemplates",
        "cleanrooms:ListCollaborationAnalysisTemplates",
        "cleanrooms:ListCollaborationConfiguredAudienceModelAssociations",
        "cleanrooms:ListCollaborations",
        "cleanrooms:ListConfiguredTableAssociations",
        "cleanrooms:ListConfiguredTables",
        "cleanrooms:ListMembers",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListProtectedQueries",
        "cleanrooms:ListSchemas",
        "cleanrooms:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CollaborationMembershipCheck",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:ListMembers"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cleanrooms-ml.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AssociateModels",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:CreateConfiguredAudienceModelAssociation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TagAssociations",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:TagResource"
      ],
      "Resource" : "arn:aws:cleanrooms:*:*:membership/*/
configuredaudiencemodelassociation/*"
    },
    {
      "Sid" : "ListRolesToPickServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetRoleAndListRolePoliciesToInspectServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/cleanrooms-ml*",
        "arn:aws:iam::*:role/role/cleanrooms-ml*"
      ]
```

```
    },
    {
      "Sid" : "ListPoliciesToInspectServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListPolicies"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetPolicyToInspectServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
      ],
      "Resource" : "arn:aws:iam::*:policy/*cleanroomsml*"
    },
    {
      "Sid" : "ConsoleDisplayTables",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetSchema",
        "glue:GetSchemaVersion",
        "glue:BatchGetPartition"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsolePickOutputBucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsolePickS3Location",
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource" : "arn:aws:s3:::*cleanrooms-ml*"
    },
    {
      "Sid" : "ConsoleDescribeECRRepositories",
      "Effect" : "Allow",
      "Action" : [
        "ecr:DescribeRepositories",
        "ecr:ListImages"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/*"
    },
    {
      "Sid" : "PassCleanRoomsResources",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:PassMembership",
        "cleanrooms:PassCollaboration"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSCleanRoomsMLReadOnlyAccess

説明: AWS Clean Rooms ML リソースへの読み取り専用アクセスと、関連する AWS Clean Rooms リソースへの読み取り専用アクセスを許可します

AWSCleanRoomsMLReadOnlyAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCleanRoomsMLReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 11 月 29 日 20:55 UTC
- 編集日時: 2025 年 1 月 10 日 20:52 UTC
- ARN: arn:aws:iam::aws:policy/AWSCleanRoomsMLReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CleanRoomsConsoleNavigation",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:GetCollaboration",
        "cleanrooms:GetConfiguredAudienceModelAssociation",
        "cleanrooms:GetMembership",
        "cleanrooms:ListAnalysisTemplates",
        "cleanrooms:ListCollaborationAnalysisTemplates",
        "cleanrooms:ListCollaborationConfiguredAudienceModelAssociations",
        "cleanrooms:ListCollaborations",
        "cleanrooms:ListConfiguredTableAssociations",
        "cleanrooms:ListConfiguredTables",
```

```
        "cleanrooms:ListMembers",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListProtectedQueries",
        "cleanrooms:ListSchemas",
        "cleanrooms:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CleanRoomsMLRead",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms-ml:Get*",
        "cleanrooms-ml:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassCleanRoomsResources",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:PassMembership",
        "cleanrooms:PassCollaboration"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSCleanRoomsReadOnlyAccess

説明: AWS Clean Rooms リソースへの読み取り専用アクセスと、関連する Glue および Amazon CloudWatch Logs AWS リソースへの読み取り専用アクセスを許可します。

AWSCleanRoomsReadOnlyAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCleanRoomsReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 1 月 12 日 16:10 UTC
- 編集日時: 2023 年 1 月 12 日 16:10 UTC
- ARN: arn:aws:iam::aws:policy/AWSCleanRoomsReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSCleanRoomsServiceRolePolicy

説明: AWS クリーンルームがユーザーに代わって CloudWatch APIs などの他の AWS サービスにアクセスすることを許可します。

AWSCleanRoomsServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2025 年 12 月 15 日 17:49 UTC
- 編集日時: 2025 年 12 月 15 日 17:49 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSCleanRoomsServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/Clean Rooms"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSCloud9Administrator

説明: AWS Cloud9 への管理者アクセスを提供します。

`AWSCloud9Administrator` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSCloud9Administrator` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 11 月 30 日 16:17 UTC
- 編集日時: 2025 年 9 月 25 日 11:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloud9Administrator`

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloud9:*",
        "iam:GetUser",
        "iam:ListUsers",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "cloud9.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession",
        "ssm:GetConnectionStatus"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
```

```
          "ssm:resourceTag/aws:cloud9:environment" : "*"
        },
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloud9.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:session/*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSCloud9EnvironmentMember

説明: AWS Cloud9 共有開発環境に招待する機能を提供します。

`AWSCloud9EnvironmentMember` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCloud9EnvironmentMember をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 11 月 30 日 16:18 UTC
- 編集日時: 2025 年 9 月 25 日 11:49 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloud9EnvironmentMember

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloud9:GetUserSettings",
        "cloud9:UpdateUserSettings",
        "cloud9:GetMigrationExperiences",
        "iam:GetUser",
        "iam:ListUsers"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloud9:DescribeEnvironmentMemberships"
      ],
```

```
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "Null" : {
          "cloud9:UserArn" : "true",
          "cloud9:EnvironmentId" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession",
        "ssm:GetConnectionStatus"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ssm:resourceTag/aws:cloud9:environment" : "*"
        },
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloud9.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:session/*"
      ]
    }
```

```
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSCloud9ServiceRolePolicy

説明: AWS Cloud9 のサービスにリンクされたロールポリシー

`AWSCloud9ServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 11 月 30 日 13:44 UTC
- 編集日時: 2022 年 1 月 17 日 14:06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCloud9ServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSCloud9SSMInstanceProfile

説明: このポリシーは、InstanceProfile にロールをアタッチするために使用され、これにより、Cloud9 は SSM Session Manager を使用してインスタンスに接続できるようになります。

`AWSCloud9SSMInstanceProfile` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSCloud9SSMInstanceProfile` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 5 月 14 日 11:40 UTC
- 編集日時: 2020 年 5 月 14 日 11:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloud9SSMInstanceProfile`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel",
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSCloud9User

説明: AWS Cloud9 開発環境を作成し、所有環境を管理するアクセス許可を提供します。

AWSCloud9User は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCloud9User をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 11 月 30 日 16:16 UTC
- 編集日時: 2025 年 9 月 25 日 11:49 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloud9User

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloud9:UpdateUserSettings",
        "cloud9:GetUserSettings",
        "cloud9:GetMigrationExperiences",
        "iam:GetUser",
        "iam:ListUsers",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "cloud9:CreateEnvironmentEC2",
        "cloud9:CreateEnvironmentSSH"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "cloud9:OwnerArn" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloud9:GetUserPublicKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "cloud9:UserArn" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloud9:DescribeEnvironmentMemberships"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "Null" : {
          "cloud9:UserArn" : "true",
          "cloud9:EnvironmentId" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "cloud9.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession",
        "ssm:GetConnectionStatus"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ssm:resourceTag/aws:cloud9:environment" : "*"
        },
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloud9.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:session/*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSCloudFormationFullAccess

説明: AWS CloudFormation へのフルアクセスを提供します。

`AWSCloudFormationFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSCloudFormationFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 7 月 26 日 21:50 UTC
- 編集日時: 2019 年 7 月 26 日 21:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudFormationFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSCloudFormationReadOnlyAccess

説明: 経由で AWS CloudFormation へのアクセスを提供します AWS マネジメントコンソール。

`AWSCloudFormationReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSCloudFormationReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:39 UTC
- 編集日時: 2019 年 11 月 13 日 17:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudFormationReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSCloudFrontLogger

説明: CloudFront Logger に CloudWatch Logs への書き込みアクセス許可を付与します。

`AWSCloudFrontLogger` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 6 月 12 日 20:15 UTC
- 編集日時: 2019 年 11 月 22 日 19:33 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCloudFrontLogger`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/cloudfront/*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSCloudFrontVPCOriginServiceRolePolicy

説明: CloudFront がユーザーに代わって EC2 Elastic Network Interfaces とセキュリティグループを管理できるようにします。

AWSCloudFrontVPCOriginServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2024 年 10 月 24 日 17:45 UTC
- 編集日時: 2024 年 10 月 24 日 17:45 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSCloudFrontVPCOriginServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
  "Statement" : [
    {
      "Sid" : "EC2Action1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/aws.cloudfront.vpcorigin" : "enabled"
        }
      },
      "Resource" : "arn:aws:ec2:*:*:network-interface/*"
    },
    {
      "Sid" : "EC2Action2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "EC2Action3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/aws.cloudfront.vpcorigin" : "enabled"
        }
      },
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "EC2Action4",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "EC2Action5",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:AssignIpv6Addresses",
        "ec2:UnassignIpv6Addresses"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/aws.cloudfront.vpcorigin" : "enabled"
        }
      },
      "Resource" : "*"
    },
    {
      "Sid" : "EC2Action6",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSubnets",
        "ec2:DescribeRegions",
        "ec2:DescribeAddresses"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2Action7",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/aws.cloudfront.vpcorigin" : "enabled",
```

```
          "ec2:CreateAction" : [
            "CreateNetworkInterface",
            "CreateSecurityGroup"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    },
    {
      "Sid" : "ElbAction1",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeTargetGroups"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSCloudHSMFullAccess

説明: すべての CloudHSM リソースへのフルアクセスを提供します。

AWSCloudHSMFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCloudHSMFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:39 UTC
- 編集日時: 2015 年 2 月 6 日 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudHSMFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSCloudHSMReadOnlyAccess

説明: すべての CloudHSM リソースへの読み取り専用アクセスを提供します。

AWSCloudHSMReadOnlyAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCloudHSMReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:39 UTC
- 編集日時: 2015 年 2 月 6 日 18:39 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloudHSMReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSCloudHSMRole

説明: AWS CloudHSM サービスロールのデフォルトポリシー。

`AWSCloudHSMRole` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSCloudHSMRole` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2015 年 2 月 6 日 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCloudHSMRole`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
```

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSCloudMapDiscoverInstanceAccess

説明: AWS クラウド Map Discovery API へのアクセスを提供します。

`AWSCloudMapDiscoverInstanceAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSCloudMapDiscoverInstanceAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 11 月 29 日 00:02 UTC
- 編集日時: 2023 年 9 月 20 日 21:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapDiscoverInstanceAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSCloudMapFullAccess

説明: すべての AWS クラウド マップアクションへのフルアクセスを提供します。

AWSCloudMapFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCloudMapFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 11 月 28 日 23:57 UTC
- 編集日時: 2020 年 7 月 29 日 19:15 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloudMapFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSCloudMapReadOnlyAccess

説明: すべての AWS クラウド Map アクションへの読み取り専用アクセスを提供します。

`AWSCloudMapReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSCloudMapReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2018 年 11 月 28 日 23:45 UTC
- 編集日時: 2023 年 9 月 20 日 21:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSCloudMapRegisterInstanceAccess

説明: Map AWS クラウド アクションへの登録者レベルのアクセスを提供します。

AWSCloudMapRegisterInstanceAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCloudMapRegisterInstanceAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 11 月 29 日 00:04 UTC
- 編集日時: 2023 年 9 月 20 日 21:47 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloudMapRegisterInstanceAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSCloudShellFullAccess

説明: すべての機能を備えた AWS CloudShell の使用を許可します

`AWSCloudShellFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSCloudShellFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 12 月 15 日 18:07 UTC
- 編集日時: 2020 年 12 月 15 日 18:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudShellFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSCloudTrail_FullAccess

説明: AWS CloudTrail へのフルアクセスを提供します。

`AWSCloudTrail_FullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSCloudTrail_FullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 10 月 8 日 23:41 UTC
- 編集日時: 2021 年 2 月 22 日 19:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudTrail_FullAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSCloudTrail_ReadOnlyAccess

説明: AWS CloudTrail への読み取り専用アクセスを提供します。

AWSCloudTrail_ReadOnlyAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCloudTrail_ReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 6 月 14 日 17:19 UTC
- 編集日時: 2022 年 6 月 14 日 17:19 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloudTrail_ReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
        "cloudtrail:List*",
        "cloudtrail:LookupEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy

説明: このポリシーは、AWSServiceRoleForCloudWatchAlarms_ActionSSMIncidents というサービスリンクロールによって使用されます。CloudWatch は、このサービスにリンクされたロールを使用して、CloudWatch アラームが ALARM 状態になったときに AWS System Manager Incident Manager アクションを実行します。このポリシーは、ユーザーに代わってインシデントを開始するアクセス許可を付与します。

`AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 4 月 27 日 13:30 UTC
- 編集日時: 2021 年 4 月 27 日 13:30 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "StartIncidentPermissions",
      "Effect" : "Allow",
      "Action" : "ssm-incidents:StartIncident",
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSCodeArtifactAdminAccess

説明: 経由で AWS CodeArtifact へのフルアクセスを提供します AWS マネジメントコンソール。

`AWSCodeArtifactAdminAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSCodeArtifactAdminAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 6 月 16 日 23:53 UTC
- 編集日時: 2020 年 6 月 16 日 23:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeArtifactAdminAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codeartifact:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "sts:GetServiceBearerToken",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "sts:AWSServiceName" : "codeartifact.amazonaws.com"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSCodeArtifactReadOnlyAccess

説明: 経由で AWS CodeArtifact への読み取り専用アクセスを提供します AWS マネジメントコンソール。

`AWSCodeArtifactReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSCodeArtifactReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 6 月 25 日 21:23 UTC
- 編集日時: 2020 年 6 月 25 日 21:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeArtifactReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
```

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSCodeBuildAdminAccess

説明: 経由で AWS CodeBuild へのフルアクセスを提供します AWS マネジメントコンソール。また、AmazonS3ReadOnlyAccess をアタッチしてビルドアーティファクトをダウンロードできるようにしたり、IAMFullAccess をアタッチして CodeBuild のサービスロールを作成および管理したりすることもできます。

AWSCodeBuildAdminAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCodeBuildAdminAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2016 年 12 月 1 日 19:04 UTC
- 編集日時: 2024 年 12 月 16 日 20:07 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeBuildAdminAccess

ポリシーのバージョン

ポリシーのバージョン: v15 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : {
        "ArnLike" : {
          "codestar-notifications:NotificationsForResource" :
"arn:aws:codebuild:*:*:project/*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
```

```
        "codestar-notifications:ListEventTypes",
        "codestar-notifications:ListTargets",
        "codestar-notifications:ListTagsforResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsSNSTopicCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:SetTopicAttributes"
      ],
      "Resource" : "arn:aws:sns:*:*:codestar-notifications*"
    },
    {
      "Sid" : "SNSTopicListAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics",
        "sns:GetTopicAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsChatbotAccess",
      "Effect" : "Allow",
      "Action" : [
        "chatbot:DescribeSlackChannelConfigurations",
        "chatbot:ListMicrosoftTeamsChannelConfigurations"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSCodeBuildDeveloperAccess

説明: 経由で AWS CodeBuild へのアクセスを提供しますが AWS マネジメントコンソール、CodeBuild プロジェクト管理は許可しません。また、AmazonS3ReadOnlyAccess をアタッチして、ビルドアーティファクトをダウンロードできるようにします。

AWSCodeBuildDeveloperAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCodeBuildDeveloperAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2016 年 12 月 1 日 19:02 UTC
- 編集日時: 2024 年 12 月 16 日 20:07 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeBuildDeveloperAccess

ポリシーのバージョン

ポリシーのバージョン: v16 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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" : {
        "ArnLike" : {
          "codestar-notifications:NotificationsForResource" :
"arn:aws:codebuild:*:*:project/*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListEventTypes",
        "codestar-notifications:ListTargets",
        "codestar-notifications:ListTagsforResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SNSTopicListAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics",
        "sns:GetTopicAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsChatbotAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "chatbot:DescribeSlackChannelConfigurations",
        "chatbot:ListMicrosoftTeamsChannelConfigurations"
      ],
      "Resource" : "*"
    }
  ],
  "Version" : "2012-10-17"
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSCodeBuildReadOnlyAccess

説明: 経由で AWS CodeBuild への読み取り専用アクセスを提供します AWS マネジメントコンソール。また、AmazonS3ReadOnlyAccess をアタッチして、ビルドアーティファクトをダウンロードできるようにします。

`AWSCodeBuildReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSCodeBuildReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2016 年 12 月 1 日 19:03 UTC
- 編集日時: 2024 年 12 月 16 日 19:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeBuildReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v13 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Statement" : [
    {
      "Sid" : "AWSServicesAccess",
      "Action" : [
        "codebuild:BatchGet*",
        "codebuild:GetResourcePolicy",
        "codebuild:List*",
        "codebuild:DescribeTestCases",
        "codebuild:DescribeCodeCoverages",
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetRepository",
        "cloudwatch:GetMetricStatistics",
        "events:DescribeRule",
        "events:ListTargetsByRule",
        "events:ListRuleNamesByTarget",
        "logs:GetLogEvents"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarConnectionsUserAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:ListConnections",
        "codestar-connections:GetConnection"
      ],
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ]
```

```
    },
    {
      "Sid" : "CodeStarNotificationsPowerUserAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:DescribeNotificationRule"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "codestar-notifications:NotificationsForResource" :
 "arn:aws:codebuild:*:*:project/*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListEventTypes",
        "codestar-notifications:ListTargets"
      ],
      "Resource" : "*"
    }
  ],
  "Version" : "2012-10-17"
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSCodeCommitFullAccess

説明: 経由で AWS CodeCommit へのフルアクセスを提供します AWS マネジメントコンソール。

`AWSCodeCommitFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCodeCommitFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 7 月 9 日 17:02 UTC
- 編集日時: 2025 年 1 月 10 日 20:07 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeCommitFullAccess

ポリシーのバージョン

ポリシーのバージョン: v11 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codecommit:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchEventsCodeCommitRulesAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:DisableRule",
        "events:EnableRule",
        "events:PutRule",
```

```
        "events:PutTargets",
        "events:RemoveTargets",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/codecommit*"
    },
    {
      "Sid" : "SNSTopicAndSubscriptionAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:DeleteTopic",
        "sns:Subscribe",
        "sns:Unsubscribe",
        "sns:SetTopicAttributes"
      ],
      "Resource" : "arn:aws:sns:*:*:codecommit*"
    },
    {
      "Sid" : "SNSTopicAndSubscriptionReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics",
        "sns:ListSubscriptionsByTopic",
        "sns:GetTopicAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LambdaReadOnlyListAccess",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMReadOnlyListAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListUsers"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "IAMReadOnlyConsoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListAccessKeys",
        "iam:ListSSHPublicKeys",
        "iam:ListServiceSpecificCredentials"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    },
    {
      "Sid" : "IAMUserSSHKeys",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteSSHPublicKey",
        "iam:GetSSHPublicKey",
        "iam:ListSSHPublicKeys",
        "iam:UpdateSSHPublicKey",
        "iam:UploadSSHPublicKey"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    },
    {
      "Sid" : "IAMSelfManageServiceSpecificCredentials",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceSpecificCredential",
        "iam:UpdateServiceSpecificCredential",
        "iam:DeleteServiceSpecificCredential",
        "iam:ResetServiceSpecificCredential"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    },
    {
      "Sid" : "CodeStarNotificationsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:CreateNotificationRule",
        "codestar-notifications:DescribeNotificationRule",
        "codestar-notifications:UpdateNotificationRule",
        "codestar-notifications:DeleteNotificationRule",
        "codestar-notifications:Subscribe",
        "codestar-notifications:Unsubscribe"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "codestar-notifications:NotificationsForResource" :
"arn:aws:codecommit:*:*:*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListTargets",
        "codestar-notifications:ListTagsforResource",
        "codestar-notifications:ListEventTypes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsSNSTopicCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:SetTopicAttributes"
      ],
      "Resource" : "arn:aws:sns:*:*:codestar-notifications*"
    },
    {
      "Sid" : "AmazonCodeGuruReviewerFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-reviewer:AssociateRepository",
        "codeguru-reviewer:DescribeRepositoryAssociation",
        "codeguru-reviewer:ListRepositoryAssociations",
        "codeguru-reviewer:DisassociateRepository",
        "codeguru-reviewer:DescribeCodeReview",
        "codeguru-reviewer:ListCodeReviews"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonCodeGuruReviewerSLRCreation",
      "Action" : "iam:CreateServiceLinkedRole",
```

```
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/codeguru-
reviewer.amazonaws.com/AWSServiceRoleForAmazonCodeGuruReviewer",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "codeguru-reviewer.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchEventsManagedRules",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:DeleteRule",
        "events:RemoveTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "codeguru-reviewer.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsChatbotAccess",
      "Effect" : "Allow",
      "Action" : [
        "chatbot:DescribeSlackChannelConfigurations",
        "chatbot:ListMicrosoftTeamsChannelConfigurations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarConnectionsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:ListConnections",
        "codestar-connections:GetConnection"
      ],
      "Resource" : "arn:aws:codestar-connections:*:*:connection/*"
    }
  ]
```

```
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSCodeCommitPowerUser

説明: AWS CodeCommit リポジトリへのフルアクセスを提供しますが、リポジトリの削除は許可しません。

`AWSCodeCommitPowerUser` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSCodeCommitPowerUser` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 7 月 9 日 17:06 UTC
- 編集日時: 2025 年 1 月 10 日 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeCommitPowerUser`

ポリシーのバージョン

ポリシーのバージョン: v16 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codecommit:AssociateApprovalRuleTemplateWithRepository",
        "codecommit:BatchAssociateApprovalRuleTemplateWithRepositories",
        "codecommit:BatchDisassociateApprovalRuleTemplateFromRepositories",
        "codecommit:BatchGet*",
        "codecommit:BatchDescribe*",
        "codecommit:Create*",
        "codecommit:DeleteBranch",
        "codecommit:DeleteFile",
        "codecommit:Describe*",
        "codecommit:DisassociateApprovalRuleTemplateFromRepository",
        "codecommit:EvaluatePullRequestApprovalRules",
        "codecommit:Get*",
        "codecommit:List*",
        "codecommit:Merge*",
        "codecommit:OverridePullRequestApprovalRules",
        "codecommit:Put*",
        "codecommit:Post*",
        "codecommit:TagResource",
        "codecommit:Test*",
        "codecommit:UntagResource",
        "codecommit:Update*",
        "codecommit:GitPull",
        "codecommit:GitPush"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchEventsCodeCommitRulesAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:DisableRule",
        "events:EnableRule",
        "events:PutRule",
```

```
        "events:PutTargets",
        "events:RemoveTargets",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/codecommit*"
    },
    {
      "Sid" : "SNSTopicAndSubscriptionAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:Subscribe",
        "sns:Unsubscribe"
      ],
      "Resource" : "arn:aws:sns:*:*:codecommit*"
    },
    {
      "Sid" : "SNSTopicAndSubscriptionReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics",
        "sns:ListSubscriptionsByTopic",
        "sns:GetTopicAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LambdaReadOnlyListAccess",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMReadOnlyListAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListUsers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMReadOnlyConsoleAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:ListAccessKeys",
        "iam:ListSSHPublicKeys",
        "iam:ListServiceSpecificCredentials"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    },
    {
      "Sid" : "IAMUserSSHKeys",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteSSHPublicKey",
        "iam:GetSSHPublicKey",
        "iam:ListSSHPublicKeys",
        "iam:UpdateSSHPublicKey",
        "iam:UploadSSHPublicKey"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    },
    {
      "Sid" : "IAMSelfManageServiceSpecificCredentials",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceSpecificCredential",
        "iam:UpdateServiceSpecificCredential",
        "iam:DeleteServiceSpecificCredential",
        "iam:ResetServiceSpecificCredential"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    },
    {
      "Sid" : "CodeStarNotificationsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:CreateNotificationRule",
        "codestar-notifications:DescribeNotificationRule",
        "codestar-notifications:UpdateNotificationRule",
        "codestar-notifications:Subscribe",
        "codestar-notifications:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
```

```
          "codestar-notifications:NotificationsForResource" :
 "arn:aws:codecommit:*:*:*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListTargets",
        "codestar-notifications:ListTagsforResource",
        "codestar-notifications:ListEventTypes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonCodeGuruReviewerFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-reviewer:AssociateRepository",
        "codeguru-reviewer:DescribeRepositoryAssociation",
        "codeguru-reviewer:ListRepositoryAssociations",
        "codeguru-reviewer:DisassociateRepository",
        "codeguru-reviewer:DescribeCodeReview",
        "codeguru-reviewer:ListCodeReviews"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonCodeGuruReviewerSLRCreation",
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/codeguru-
reviewer.amazonaws.com/AWSServiceRoleForAmazonCodeGuruReviewer",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "codeguru-reviewer.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchEventsManagedRules",
      "Effect" : "Allow",
```

```
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:DeleteRule",
        "events:RemoveTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "codeguru-reviewer.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsChatbotAccess",
      "Effect" : "Allow",
      "Action" : [
        "chatbot:DescribeSlackChannelConfigurations",
        "chatbot:ListMicrosoftTeamsChannelConfigurations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarConnectionsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:ListConnections",
        "codestar-connections:GetConnection"
      ],
      "Resource" : "arn:aws:codestar-connections:*:*:connection/*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSCodeCommitReadOnly

説明: 経由で AWS CodeCommit への読み取り専用アクセスを提供します AWS マネジメントコンソール。

AWSCodeCommitReadOnly は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCodeCommitReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 7 月 9 日 17:05 UTC
- 編集日時: 2025 年 1 月 10 日 20:07 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeCommitReadOnly

ポリシーのバージョン

ポリシーのバージョン: v12 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codecommit:BatchGet*",
        "codecommit:BatchDescribe*",
        "codecommit:Describe*",
        "codecommit:EvaluatePullRequestApprovalRules",
        "codecommit:Get*",
        "codecommit:List*",
```

```
        "codecommit:GitPull"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchEventsCodeCommitRulesReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/codecommit*"
    },
    {
      "Sid" : "SNSSubscriptionAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics",
        "sns:ListSubscriptionsByTopic",
        "sns:GetTopicAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LambdaReadOnlyListAccess",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMReadOnlyListAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListUsers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMReadOnlyConsoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListSSHPublicKeys",
```

```
        "iam:ListServiceSpecificCredentials",
        "iam:ListAccessKeys",
        "iam:GetSSHPublicKey"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    },
    {
      "Sid" : "CodeStarConnectionsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:ListConnections",
        "codestar-connections:GetConnection"
      ],
      "Resource" : "arn:aws:codestar-connections:*:*:connection/*"
    },
    {
      "Sid" : "CodeStarNotificationsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:DescribeNotificationRule"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "codestar-notifications:NotificationsForResource" :
"arn:aws:codecommit:*:*:*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListEventTypes",
        "codestar-notifications:ListTargets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonCodeGuruReviewerReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-reviewer:DescribeRepositoryAssociation",
```

```
        "codeguru-reviewer:ListRepositoryAssociations",
        "codeguru-reviewer:DescribeCodeReview",
        "codeguru-reviewer:ListCodeReviews"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSCodeDeployDeployerAccess

説明: リビジョンを登録してデプロイするためのアクセスを提供します。

AWSCodeDeployDeployerAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCodeDeployDeployerAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 5 月 19 日 18:18 UTC
- 編集日時: 2024 年 12 月 16 日 20:22 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeDeployDeployerAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codedeploy:Batch*",
        "codedeploy:CreateDeployment",
        "codedeploy:Get*",
        "codedeploy:List*",
        "codedeploy:RegisterApplicationRevision"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:CreateNotificationRule",
        "codestar-notifications:DescribeNotificationRule",
        "codestar-notifications:UpdateNotificationRule",
        "codestar-notifications:Subscribe",
        "codestar-notifications:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "codestar-notifications:NotificationsForResource" :
 "arn:aws:codedeploy:*:*:application:*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
```

```
        "codestar-notifications:ListTargets",
        "codestar-notifications:ListTagsforResource",
        "codestar-notifications:ListEventTypes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsChatbotAccess",
      "Effect" : "Allow",
      "Action" : [
        "chatbot:DescribeSlackChannelConfigurations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SNSTopicListAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSCodeDeployFullAccess

説明: CodeDeploy リソースへのフルアクセスを提供します。

`AWSCodeDeployFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSCodeDeployFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 5 月 19 日 18:13 UTC
- 編集日時: 2024 年 12 月 16 日 20:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : "codedeploy:*",
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:CreateNotificationRule",
        "codestar-notifications:DescribeNotificationRule",
        "codestar-notifications:UpdateNotificationRule",
        "codestar-notifications:DeleteNotificationRule",
        "codestar-notifications:Subscribe",
        "codestar-notifications:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
```

```
          "codestar-notifications:NotificationsForResource" :
 "arn:aws:codedeploy:*:*:application:*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListTargets",
        "codestar-notifications:ListTagsforResource",
        "codestar-notifications:ListEventTypes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsSNSTopicCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:SetTopicAttributes"
      ],
      "Resource" : "arn:aws:sns:*:*:codestar-notifications*"
    },
    {
      "Sid" : "CodeStarNotificationsChatbotAccess",
      "Effect" : "Allow",
      "Action" : [
        "chatbot:DescribeSlackChannelConfigurations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SNSTopicListAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSCodeDeployReadOnlyAccess

説明: CodeDeploy リソースへの読み取り専用アクセスを提供します。

AWSCodeDeployReadOnlyAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCodeDeployReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 5 月 19 日 18:21 UTC
- 編集日時: 2024 年 12 月 16 日 20:07 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeDeployReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
    {
      "Action" : [
        "codedeploy:Batch*",
        "codedeploy:Get*",
        "codedeploy:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsPowerUserAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:DescribeNotificationRule"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "codestar-notifications:NotificationsForResource" :
 "arn:aws:codedeploy:*:*:application:*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListEventTypes",
        "codestar-notifications:ListTargets"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSCodeDeployRole

説明: CodeDeploy サービスに、ユーザーに代わってタグを拡張し自動スケーリングとやり取りする許可を付与します。

AWSCodeDeployRole は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCodeDeployRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 5 月 4 日 18:05 UTC
- 編集日時: 2023 年 8 月 16 日 20:38 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSCodeDeployRole

ポリシーのバージョン

ポリシーのバージョン: v11 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する

- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSCodeDeployRoleForCloudFormation

説明: CodeDeploy サービスに、ユーザーに代わって Lambda 関数を呼び出し、CloudFormation 経由でブルー/グリーンデプロイを実行するためのアクセスを提供します。

AWSCodeDeployRoleForCloudFormation は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCodeDeployRoleForCloudFormation をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 5 月 19 日 17:12 UTC
- 編集日時: 2020 年 5 月 19 日 17:12 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForCloudFormation

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:CodeDeployHook_*",
      "Effect" : "Allow"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSCodeDeployRoleForECS

説明: CodeDeploy サービスに、ユーザーに代わって ECS ブルー/グリーンデプロイを実行するための広範なアクセスを提供します。すべての S3 オブジェクトの読み取り、すべての Lambda 関数の呼び出し、アカウント内のすべての SNS トピックへの公開、すべての ECS サービスの更新など、サポートサービスへのフルアクセスを許可します。

AWSCodeDeployRoleForECS は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCodeDeployRoleForECS をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 11 月 27 日 20:40 UTC
- 編集日時: 2019 年 9 月 23 日 22:37 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSCodeDeployRoleForECSLimited

説明: CodeDeploy サービスに、ユーザーに代わって ECS ブルー/グリーンデプロイを実行するための限定アクセスを提供します。

`AWSCodeDeployRoleForECSLimited` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSCodeDeployRoleForECSLimited` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 11 月 27 日 20:42 UTC
- 編集日時: 2019 年 9 月 23 日 22:10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployRoleForECSLimited`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSCodeDeployRoleForLambda

説明: CodeDeploy サービスに、ユーザーに代わって Lambda デプロイを実行するためのアクセスを提供します。

AWSCodeDeployRoleForLambda は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCodeDeployRoleForLambda をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2017 年 11 月 28 日 14:05 UTC
- 編集日時: 2019 年 12 月 3 日 19:53 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForLambda

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSCodeDeployRoleForLambdaLimited

説明: CodeDeploy サービスに、ユーザーに代わって Lambda デプロイを実行するための制限付きアクセス権を提供します。

AWSCodeDeployRoleForLambdaLimited は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCodeDeployRoleForLambdaLimited をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 8 月 17 日 17:14 UTC
- 編集日時: 2020 年 8 月 17 日 17:14 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForLambdaLimited

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSCodePipeline_FullAccess

説明: 経由で AWS CodePipeline へのフルアクセスを提供します AWS マネジメントコンソール。

AWSCodePipeline_FullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCodePipeline_FullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 8 月 3 日 22:38 UTC
- 編集日時: 2024 年 3 月 14 日 17:06 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodePipeline_FullAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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"
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSCodePipeline_ReadOnlyAccess

説明: 経由で AWS CodePipeline への読み取り専用アクセスを提供します AWS マネジメントコンソール。

`AWSCodePipeline_ReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSCodePipeline_ReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 8 月 3 日 22:25 UTC
- 編集日時: 2020 年 8 月 3 日 22:25 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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"
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSCodePipelineApproverAccess

説明: すべてのパイプラインの手動変更を確認および承認するためのアクセスを提供します

AWSCodePipelineApproverAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCodePipelineApproverAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2016 年 7 月 28 日 18:59 UTC
- 編集日時: 2017 年 8 月 2 日 17:24 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodePipelineApproverAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:GetPipelineExecution",
        "codepipeline:ListPipelineExecutions",
        "codepipeline:ListPipelines",
        "codepipeline:PutApprovalResult"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSCodePipelineCustomActionAccess

説明: ジョブの詳細 (一時的な認証情報を含む) をポーリングし、 AWS CodePipeline のステータス更新をレポートするカスタムアクションへのアクセスを提供します。

AWSCodePipelineCustomActionAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCodePipelineCustomActionAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 7 月 9 日 17:02 UTC
- 編集日時: 2015 年 7 月 9 日 17:02 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodePipelineCustomActionAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Statement" : [
    {
      "Action" : [
        "codepipeline:AcknowledgeJob",
        "codepipeline:GetJobDetails",
        "codepipeline:PollForJobs",
        "codepipeline:PutJobFailureResult",
        "codepipeline:PutJobSuccessResult"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ],
  "Version" : "2012-10-17"
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSCodeStarFullAccess

説明: 経由で AWS CodeStar へのフルアクセスを提供します AWS マネジメントコンソール。

`AWSCodeStarFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSCodeStarFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 4 月 19 日 16:23 UTC
- 編集日時: 2023 年 3 月 28 日 00:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeStarFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSCodeStarNotificationsServiceRolePolicy

説明: ユーザーに代わって Amazon CloudWatch Events にアクセスするための Allow AWS CodeStar Notifications

`AWSCodeStarNotificationsServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 11 月 5 日 16:10 UTC
- 編集日時: 2020 年 3 月 19 日 16:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCodeStarNotificationsServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSCodeStarServiceRole

説明: 使用しないでください。この AWS CodeStar サービスロールポリシーは、CodeStar がお客様に代わって IAM やその他のサービスリソースを管理するための管理者権限を付与するものです。

AWSCodeStarServiceRole は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCodeStarServiceRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2017 年 4 月 19 日 15:20 UTC
- 編集日時: 2021 年 9 月 20 日 19:11 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSCodeStarServiceRole

ポリシーのバージョン

ポリシーのバージョン: v11 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSCompromisedKeyQuarantine

説明: IAM ユーザーの認証情報が侵害または公開された場合に AWS チームによって適用される特定のアクションへのアクセスを拒否します。このポリシーは削除しないでください。代わりに、このイベントに関して送信されたメールで指示されている手順に従ってください。

`AWSCompromisedKeyQuarantine` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSCompromisedKeyQuarantine` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 8 月 11 日 18:04 UTC
- 編集日時: 2020 年 8 月 11 日 18:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCompromisedKeyQuarantine`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント


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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSCompromisedKeyQuarantineV2

説明: IAM ユーザーの認証情報が侵害または公開された場合に AWS チームによって適用される特定のアクションへのアクセスを拒否します。このポリシーは削除しないでください。代わりに、このイベントに関して作成したサポートケースに明記されている指示に従ってください。

`AWSCompromisedKeyQuarantineV2` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSCompromisedKeyQuarantineV2` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 4 月 21 日 22:30 UTC
- 編集日時: 2024 年 10 月 2 日 16:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCompromisedKeyQuarantineV2`

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Deny",
      "Action" : [
        "cloudtrail:LookupEvents",
        "ec2:RequestSpotInstances",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "iam:AddUserToGroup",
        "iam:AttachGroupPolicy",
        "iam:AttachRolePolicy",
        "iam:AttachUserPolicy",
        "iam:ChangePassword",
        "iam:CreateAccessKey",
        "iam:CreateInstanceProfile",
        "iam:CreateLoginProfile",
        "iam:CreatePolicyVersion",
        "iam:CreateRole",
        "iam:CreateUser",
        "iam:DetachUserPolicy",
        "iam:PassRole",
        "iam:PutGroupPolicy",
        "iam:PutRolePolicy",
        "iam:PutUserPermissionsBoundary",
        "iam:PutUserPolicy",
        "iam:SetDefaultPolicyVersion",
        "iam:UpdateAccessKey",
        "iam:UpdateAccountPasswordPolicy",
        "iam:UpdateAssumeRolePolicy",
        "iam:UpdateLoginProfile",
        "iam:UpdateUser",
        "lambda:AddLayerVersionPermission",
        "lambda:AddPermission",
        "lambda:CreateFunction",
        "lambda:GetPolicy",
```

```
        "lambda:ListTags",
        "lambda:PutProvisionedConcurrencyConfig",
        "lambda:TagResource",
        "lambda:UntagResource",
        "lambda:UpdateFunctionCode",
        "lightsail:Create*",
        "lightsail:Delete*",
        "lightsail:DownloadDefaultKeyPair",
        "lightsail:GetInstanceAccessDetails",
        "lightsail:Start*",
        "lightsail:Update*",
        "organizations:CreateAccount",
        "organizations:CreateOrganization",
        "organizations:InviteAccountToOrganization",
        "s3:DeleteBucket",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketAcl",
        "s3:PutBucketOwnershipControls",
        "s3:DeleteBucketPolicy",
        "s3:ObjectOwnerOverrideToBucketOwner",
        "s3:PutAccountPublicAccessBlock",
        "s3:PutBucketPolicy",
        "s3:ListAllMyBuckets",
        "ec2:PurchaseReservedInstancesOffering",
        "ec2:AcceptReservedInstancesExchangeQuote",
        "ec2:CreateReservedInstancesListing",
        "savingsplans:CreateSavingsPlan",
        "ecs:CreateService",
        "ecs:CreateCluster",
        "ecs:RegisterTaskDefinition",
        "ecr:GetAuthorizationToken",
        "bedrock:CreateModelInvocationJob",
        "bedrock:InvokeModelWithResponseStream",
        "bedrock:CreateFoundationModelAgreement",
        "bedrock:PutFoundationModelEntitlement",
        "bedrock:InvokeModel",
        "s3:CreateBucket",
        "s3:PutBucketCors",
        "s3:GetObject",
        "s3:ListBucket",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateProcessingJob",
```

```
        "ses:GetSendQuota",
        "ses:ListIdentities",
        "sts:GetSessionToken",
        "sts:GetFederationToken",
        "amplify:CreateDeployment",
        "amplify:CreateBackendEnvironment",
        "codebuild:CreateProject",
        "glue:CreateJob",
        "iam:DeleteRole",
        "iam:DeleteAccessKey",
        "iam:ListUsers",
        "lambda:GetEventSourceMapping",
        "sns:GetSMSAttributes",
        "mediapackagev2:CreateChannel"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSCompromisedKeyQuarantineV3

説明: IAM ユーザーの認証情報 AWS が侵害または公開された場合に によって適用される特定のアクションへのアクセスを拒否します。このポリシーは、既存のリソースに影響を与えずに、不正請求につながる詐欺行為によって発生する損害を制限することを目的としています。このポリシーは削除しないでください。代わりに、このイベントに関して作成したサポートケースに明記されている指示に従ってください。

AWSCompromisedKeyQuarantineV3 は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCompromisedKeyQuarantineV3 をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 8 月 21 日 17:36 UTC
- 編集日時: 2024 年 10 月 2 日 16:52 UTC
- ARN: arn:aws:iam::aws:policy/AWSCompromisedKeyQuarantineV3

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Deny",
      "Action" : [
        "cloudtrail:LookupEvents",
        "ec2:RequestSpotInstances",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "iam:AddUserToGroup",
        "iam:AttachGroupPolicy",
        "iam:AttachRolePolicy",
        "iam:AttachUserPolicy",
        "iam:ChangePassword",
        "iam:CreateAccessKey",
        "iam:CreateInstanceProfile",
        "iam:CreateLoginProfile",
        "iam:CreatePolicyVersion",
```

```
        "iam:CreateRole",
        "iam:CreateUser",
        "iam:DetachUserPolicy",
        "iam:PassRole",
        "iam:PutGroupPolicy",
        "iam:PutRolePolicy",
        "iam:PutUserPermissionsBoundary",
        "iam:PutUserPolicy",
        "iam:SetDefaultPolicyVersion",
        "iam:UpdateAccessKey",
        "iam:UpdateAccountPasswordPolicy",
        "iam:UpdateAssumeRolePolicy",
        "iam:UpdateLoginProfile",
        "iam:UpdateUser",
        "lambda:AddLayerVersionPermission",
        "lambda:AddPermission",
        "lambda:CreateFunction",
        "lambda:GetPolicy",
        "lambda:ListTags",
        "lambda:PutProvisionedConcurrencyConfig",
        "lambda:TagResource",
        "lambda:UntagResource",
        "lambda:UpdateFunctionCode",
        "lightsail:Create*",
        "lightsail:Delete*",
        "lightsail:DownloadDefaultKeyPair",
        "lightsail:GetInstanceAccessDetails",
        "lightsail:Start*",
        "lightsail:Update*",
        "organizations:CreateAccount",
        "organizations:CreateOrganization",
        "organizations:InviteAccountToOrganization",
        "s3:DeleteBucket",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketAcl",
        "s3:PutBucketOwnershipControls",
        "s3:DeleteBucketPolicy",
        "s3:ObjectOwnerOverrideToBucketOwner",
        "s3:PutAccountPublicAccessBlock",
        "s3:PutBucketPolicy",
        "s3:ListAllMyBuckets",
        "ec2:PurchaseReservedInstancesOffering",
```

```
        "ec2:AcceptReservedInstancesExchangeQuote",
        "ec2:CreateReservedInstancesListing",
        "savingsplans:CreateSavingsPlan",
        "ecs:CreateService",
        "ecs:CreateCluster",
        "ecs:RegisterTaskDefinition",
        "ecr:GetAuthorizationToken",
        "bedrock:CreateModelInvocationJob",
        "bedrock:InvokeModelWithResponseStream",
        "bedrock:CreateFoundationModelAgreement",
        "bedrock:PutFoundationModelEntitlement",
        "bedrock:InvokeModel",
        "s3:CreateBucket",
        "s3:PutBucketCors",
        "s3:GetObject",
        "s3:ListBucket",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateProcessingJob",
        "ses:GetSendQuota",
        "ses:ListIdentities",
        "sts:GetSessionToken",
        "sts:GetFederationToken",
        "amplify:CreateDeployment",
        "amplify:CreateBackendEnvironment",
        "codebuild:CreateProject",
        "glue:CreateJob",
        "iam:DeleteRole",
        "iam:DeleteAccessKey",
        "iam:ListUsers",
        "lambda:GetEventSourceMapping",
        "sns:GetSMSAttributes",
        "mediapackagev2:CreateChannel"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する

- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSConfigMultiAccountSetupPolicy

説明: Config が AWS サービスを呼び出し、組織全体に Config リソースをデプロイすることを許可する

AWSConfigMultiAccountSetupPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 6 月 17 日 18:03 UTC
- 編集日時: 2023 年 2 月 24 日 01:39 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSConfigMultiAccountSetupPolicy

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSConfigRemediationServiceRolePolicy

説明: AWS Config がユーザーに代わって非準拠のリソースを修復できるようにします。

AWSConfigRemediationServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 6 月 18 日 21:21 UTC
- 編集日時: 2019 年 6 月 18 日 21:21 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSConfigRemediationServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSConfigRoleForOrganizations

説明: Config AWS が読み取り専用 AWS Organizations APIs を呼び出すことを許可します

AWSConfigRoleForOrganizations は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSConfigRoleForOrganizations をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2018 年 3 月 19 日 22:53 UTC
- 編集日時: 2020 年 11 月 24 日 20:19 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSConfigRoleForOrganizations

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSConfigRulesExecutionRole

説明: AWS Lambda 関数が Config API AWS および Config が Amazon S3 AWS に定期的に配信する設定スナップショットにアクセスできるようにします。このアクセスは、カスタム Config ルールの設定変更を評価する関数に必要です。

`AWSConfigRulesExecutionRole` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSConfigRulesExecutionRole` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2016 年 3 月 25 日 17:59 UTC
- 編集日時: 2019 年 5 月 13 日 21:33 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSConfigRulesExecutionRole`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSConfigServiceRolePolicy

説明: Config がユーザーに代わって AWS サービスを呼び出し、リソース設定を収集できるようにします。

AWSConfigServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 5 月 30 日 23:31 UTC
- 編集日時: 2025 年 11 月 21 日 17:04 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSConfigServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v63 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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:GetAccountConfiguration",
        "acm:ListCertificates",
        "acm:ListTagsForCertificate",
        "airflow:GetEnvironment",
        "airflow:ListEnvironments",
        "airflow:ListTagsForResource",
        "amplify:GetApp",
        "amplify:GetBranch",
        "amplify:GetDomainAssociation",
        "amplify:ListApps",
        "amplify:ListBranches",
        "amplify:ListDomainAssociations",
        "amplify:ListTagsForResource",
        "amplifyuibuilder:ExportThemes",
        "amplifyuibuilder:GetTheme",
        "amplifyuibuilder:ListForms",
        "amplifyuibuilder:ListThemes",
        "aoss:BatchGetCollection",
        "aoss:BatchGetLifecyclePolicy",
        "aoss:BatchGetVpcEndpoint",
        "aoss:GetAccessPolicy",
        "aoss:GetSecurityConfig",
```

```
            "aoss:GetSecurityPolicy",
            "aoss:ListAccessPolicies",
            "aoss:ListCollections",
            "aoss:ListLifecyclePolicies",
            "aoss:ListSecurityConfigs",
            "aoss:ListSecurityPolicies",
            "aoss:ListVpcEndpoints",
            "app-integrations:GetApplication",
            "app-integrations:GetDataIntegration",
            "app-integrations:GetEventIntegration",
            "app-integrations:ListApplications",
            "app-integrations:ListDataIntegrations",
            "app-integrations:ListEventIntegrationAssociations",
            "app-integrations:ListEventIntegrations",
            "app-integrations:ListTagsForResource",
            "appconfig:GetApplication",
            "appconfig:GetConfigurationProfile",
            "appconfig:GetDeployment",
            "appconfig:GetDeploymentStrategy",
            "appconfig:GetEnvironment",
            "appconfig:GetExtension",
            "appconfig:GetExtensionAssociation",
            "appconfig:GetHostedConfigurationVersion",
            "appconfig:ListApplications",
            "appconfig:ListConfigurationProfiles",
            "appconfig:ListDeployments",
            "appconfig:ListDeploymentStrategies",
            "appconfig:ListEnvironments",
            "appconfig:ListExtensionAssociations",
            "appconfig:ListExtensions",
            "appconfig:ListHostedConfigurationVersions",
            "appconfig:ListTagsForResource",
            "appflow:DescribeConnectorProfiles",
            "appflow:DescribeFlow",
            "appflow:ListFlows",
            "appflow:ListTagsForResource",
            "application-autoscaling:DescribeScalableTargets",
            "application-autoscaling:DescribeScalingPolicies",
            "application-signals:GetServiceLevelObjective",
            "application-signals:ListServiceLevelObjectiveExclusionWindows",
            "application-signals:ListServiceLevelObjectives",
            "application-signals:ListTagsForResource",
            "appmesh:DescribeGatewayRoute",
            "appmesh:DescribeMesh",
```

```
        "appmesh:DescribeRoute",
        "appmesh:DescribeVirtualGateway",
        "appmesh:DescribeVirtualNode",
        "appmesh:DescribeVirtualRouter",
        "appmesh:DescribeVirtualService",
        "appmesh:ListGatewayRoutes",
        "appmesh:ListMeshes",
        "appmesh:ListRoutes",
        "appmesh:ListTagsForResource",
        "appmesh:ListVirtualGateways",
        "appmesh:ListVirtualNodes",
        "appmesh:ListVirtualRouters",
        "appmesh:ListVirtualServices",
        "apprunner:DescribeObservabilityConfiguration",
        "apprunner:DescribeService",
        "apprunner:DescribeVpcConnector",
        "apprunner:DescribeVpcIngressConnection",
        "apprunner:ListObservabilityConfigurations",
        "apprunner:ListServices",
        "apprunner:ListTagsForResource",
        "apprunner:ListVpcConnectors",
        "appstream:DescribeAppBlockBuilders",
        "appstream:DescribeApplications",
        "appstream:DescribeDirectoryConfigs",
        "appstream:DescribeFleets",
        "appstream:DescribeStacks",
        "appstream:ListTagsForResource",
        "appsync:GetApiCache",
        "appsync:GetGraphqlApi",
        "appsync:GetSourceApiAssociation",
        "appsync:ListGraphqlApis",
        "appsync:ListSourceApiAssociations",
        "aps:DescribeAlertManagerDefinition",
        "aps:DescribeLoggingConfiguration",
        "APS:DescribeRuleGroupsNamespace",
        "APS:DescribeWorkspace",
        "aps:ListRuleGroupsNamespaces",
        "aps:ListTagsForResource",
        "APS:ListWorkspaces",
        "apprunner:DescribeAutoScalingConfiguration",
        "apprunner:ListAutoScalingConfigurations",
        "apprunner:ListVpcIngressConnections",
        "appstream:DescribeAppBlocks",
        "appstream:DescribeImageBuilders",
```

```
        "appsync:GetApi",
        "appsync:GetDomainName",
        "appsync:ListApis",
        "appsync:ListDomainNames",
        "appsync:ListTagsForResource",
        "apptest:GetTestCase",
        "apptest:ListTagsForResource",
        "apptest:ListTestCases",
        "aps:DescribeScraper",
        "aps:DescribeScraperLoggingConfiguration",
        "aps:ListScrapers",
        "arc-zonal-shift:GetAutoshiftObserverNotificationStatus",
        "athena:GetDataCatalog",
        "athena:GetPreparedStatement",
        "athena:GetWorkGroup",
        "athena:ListDataCatalogs",
        "athena:ListPreparedStatements",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups",
        "auditmanager:GetAccountStatus",
        "auditmanager:GetAssessment",
        "auditmanager:ListAssessments",
        "autoscaling-plans:DescribeScalingPlanResources",
        "autoscaling-plans:DescribeScalingPlans",
        "autoscaling-plans:GetScalingPlanResourceForecastData",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeLaunchConfigurations",
        "autoscaling:DescribeLifecycleHooks",
        "autoscaling:DescribePolicies",
        "autoscaling:DescribeScheduledActions",
        "autoscaling:DescribeTags",
        "autoscaling:DescribeWarmPool",
        "b2bi:GetCapability",
        "b2bi:GetPartnership",
        "b2bi:GetProfile",
        "b2bi:GetTransformer",
        "b2bi:ListCapabilities",
        "b2bi:ListPartnerships",
        "b2bi:ListProfiles",
        "b2bi:ListTagsForResource",
        "b2bi:ListTransformers",
        "backup-gateway:GetHypervisor",
        "backup-gateway:ListHypervisors",
        "backup-gateway:ListTagsForResource",
```

```
        "backup-gateway:ListVirtualMachines",
        "backup:DescribeBackupVault",
        "backup:DescribeFramework",
        "backup:DescribeProtectedResource",
        "backup:DescribeRecoveryPoint",
        "backup:DescribeReportPlan",
        "backup:GetBackupPlan",
        "backup:GetBackupSelection",
        "backup:GetBackupVaultAccessPolicy",
        "backup:GetBackupVaultNotifications",
        "backup:GetRestoreTestingPlan",
        "backup:GetRestoreTestingSelection",
        "backup:ListBackupPlans",
        "backup:ListBackupSelections",
        "backup:ListBackupVaults",
        "backup:ListFrameworks",
        "backup:ListRecoveryPointsByBackupVault",
        "backup:ListReportPlans",
        "backup:ListRestoreTestingPlans",
        "backup:ListRestoreTestingSelections",
        "backup:ListTags",
        "batch:DescribeComputeEnvironments",
        "batch:DescribeJobQueues",
        "batch:DescribeSchedulingPolicies",
        "batch:ListSchedulingPolicies",
        "batch:ListTagsForResource",
        "bcm-data-exports:GetExport",
        "bcm-data-exports:ListExports",
        "bcm-data-exports:ListTagsForResource",
        "bedrock-agentcore:GetAgentRuntime",
        "bedrock-agentcore:GetAgentRuntimeEndpoint",
        "bedrock-agentcore:GetBrowser",
        "bedrock-agentcore:GetCodeInterpreter",
        "bedrock-agentcore:ListAgentRuntimeEndpoints",
        "bedrock-agentcore:ListAgentRuntimes",
        "bedrock-agentcore:ListBrowsers",
        "bedrock-agentcore:ListCodeInterpreters",
        "bedrock-agentcore:ListTagsForResource",
        "bedrock:GetAgent",
        "bedrock:GetAgentActionGroup",
        "bedrock:GetAgentAlias",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:GetDataAutomationProject",
        "bedrock:GetDataSource",
```

```
        "bedrock:GetFlow",
        "bedrock:GetFlowAlias",
        "bedrock:GetFlowVersion",
        "bedrock:GetGuardrail",
        "bedrock:GetInferenceProfile",
        "bedrock:GetKnowledgeBase",
        "bedrock:GetModelInvocationLoggingConfiguration",
        "bedrock:ListAgentActionGroups",
        "bedrock:ListAgentAliases",
        "bedrock:ListAgentCollaborators",
        "bedrock:ListAgentKnowledgeBases",
        "bedrock:ListAgents",
        "bedrock:ListDataAutomationProjects",
        "bedrock:ListDataSources",
        "bedrock:ListFlowAliases",
        "bedrock:ListFlowVersions",
        "bedrock:ListFlows",
        "bedrock:ListGuardrails",
        "bedrock:ListInferenceProfiles",
        "bedrock:ListKnowledgeBases",
        "bedrock:ListPrompts",
        "bedrock:ListTagsForResource",
        "billingconductor:ListAccountAssociations",
        "billingconductor:ListBillingGroups",
        "billingconductor:ListCustomLineItems",
        "billingconductor:ListPricingPlans",
        "billingconductor:ListPricingRules",
        "billingconductor:ListPricingRulesAssociatedToPricingPlan",
        "billingconductor:ListTagsForResource",
        "budgets:DescribeBudgetAction",
        "budgets:DescribeBudgetActionsForAccount",
        "budgets:DescribeBudgetActionsForBudget",
        "budgets:ViewBudget",
        "cassandra:Select",
        "ce:DescribeCostCategoryDefinition",
        "ce:GetAnomalyMonitors",
        "ce:GetAnomalySubscriptions",
        "ce:ListCostCategoryDefinitions",
        "ce:ListTagsForResource",
        "cleanrooms-ml:GetTrainingDataset",
        "cleanrooms-ml:ListTrainingDatasets",
        "cleanrooms:GetAnalysisTemplate",
        "cleanrooms:GetConfiguredTable",
        "cleanrooms:GetConfiguredTableAnalysisRule",
```

```
        "cleanrooms:GetMembership",
        "cleanrooms:GetPrivacyBudgetTemplate",
        "cleanrooms:ListAnalysisTemplates",
        "cleanrooms:ListConfiguredTables",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListPrivacyBudgetTemplates",
        "cleanrooms:ListTagsForResource",
        "cloud9:DescribeEnvironmentMemberships",
        "cloud9:DescribeEnvironments",
        "cloud9:ListEnvironments",
        "cloud9:ListTagsForResource",
        "cloudformation:BatchDescribeTypeConfigurations",
        "cloudformation:DescribePublisher",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeType",
        "cloudformation:GetResource",
        "cloudformation:ListResources",
        "cloudformation:ListStackInstances",
        "cloudformation:ListStackResources",
        "cloudformation:ListStacks",
        "cloudformation:ListStackSets",
        "cloudformation:ListTypes",
        "cloudfront:DescribeFunction",
        "cloudfront:DescribeKeyValueStore",
        "cloudfront:GetConnectionGroup",
        "cloudfront:GetFunction",
        "cloudfront:GetOriginAccessControl",
        "cloudfront:GetPublicKey",
        "cloudfront:GetRealtimeLogConfig",
        "cloudfront:GetResponseHeadersPolicy",
        "cloudfront:ListDistributions",
        "cloudfront:ListFunctions",
        "cloudfront:ListOriginAccessControls",
        "cloudfront:ListPublicKeys",
        "cloudfront:ListRealtimeLogConfigs",
        "cloudfront:ListResponseHeadersPolicies",
        "cloudfront:ListTagsForResource",
        "cloudtrail:DescribeTrails",
        "cloudTrail:GetChannel",
        "cloudtrail:GetEventConfiguration",
        "cloudtrail:GetEventDataStore",
        "cloudtrail:GetEventSelectors",
        "cloudtrail:GetInsightSelectors",
```

```
        "cloudtrail:GetResourcePolicy",
        "cloudtrail:GetTrailStatus",
        "cloudTrail:ListChannels",
        "cloudfront:GetDistributionTenant",
        "cloudfront:GetVpcOrigin",
        "cloudfront:ListConnectionGroups",
        "cloudfront:ListDistributionTenants",
        "cloudfront:ListKeyValueStores",
        "cloudfront:ListVpcOrigins",
        "cloudtrail:GetDashboard",
        "cloudtrail:ListDashboards",
        "cloudtrail:ListEventDataStores",
        "cloudtrail:ListTags",
        "cloudtrail:ListTrails",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:DescribeAnomalyDetectors",
        "cloudwatch:GetDashboard",
        "cloudwatch:GetMetricStream",
        "cloudwatch:ListDashboards",
        "cloudwatch:ListMetricStreams",
        "cloudwatch:ListTagsForResource",
        "codeartifact:DescribeDomain",
        "codeartifact:DescribePackageGroup",
        "codeartifact:DescribeRepository",
        "codeartifact:GetDomainPermissionsPolicy",
        "codeartifact:GetRepositoryPermissionsPolicy",
        "codeartifact:ListAllowedRepositoriesForGroup",
        "codeartifact:ListDomains",
        "codeartifact:ListPackageGroups",
        "codeartifact:ListPackages",
        "codeartifact:ListPackageVersions",
        "codeartifact:ListRepositories",
        "codeartifact:ListTagsForResource",
        "codebuild:BatchGetReportGroups",
        "codebuild:ListReportGroups",
        "codecommit:GetRepository",
        "codecommit:GetRepositoryTriggers",
        "codecommit:ListRepositories",
        "codecommit:ListTagsForResource",
        "codeconnections:GetConnection",
        "codeconnections:ListConnections",
        "codeconnections:ListTagsForResource",
        "codedeploy:GetDeploymentConfig",
```

```
        "codeguru-profiler:DescribeProfilingGroup",
        "codeguru-profiler:GetNotificationConfiguration",
        "codeguru-profiler:GetPolicy",
        "codeguru-profiler:ListProfilingGroups",
        "codeguru-reviewer:DescribeRepositoryAssociation",
        "codeguru-reviewer:ListRepositoryAssociations",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:ListActionTypes",
        "codepipeline:ListPipelines",
        "codepipeline:ListTagsForResource",
        "codepipeline:ListWebhooks",
        "codestar-connections:GetConnection",
        "codestar-connections:GetRepositoryLink",
        "codestar-connections:ListConnections",
        "codestar-connections:ListRepositoryLinks",
        "codestar-connections:ListTagsForResource",
        "cognito-identity:DescribeIdentityPool",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:GetPrincipalTagAttributeMap",
        "cognito-identity:ListIdentityPools",
        "cognito-identity:ListTagsForResource",
        "cognito-idp: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",
        "comprehend:DescribeFlywheel",
        "comprehend:ListFlywheels",
        "comprehend:ListTagsForResource",
        "config:BatchGet*",
        "config:Describe*",
        "config:Get*",
        "config:List*",
        "config:Put*",
        "config:Select*",
```

```
        "connect:DescribeEvaluationForm",
        "connect:DescribeInstance",
        "connect:DescribeInstanceStorageConfig",
        "connect:DescribePhoneNumber",
        "connect:DescribePredefinedAttribute",
        "connect:DescribePrompt",
        "connect:DescribeQueue",
        "connect:DescribeQuickConnect",
        "connect:DescribeRoutingProfile",
        "connect:DescribeRule",
        "connect:DescribeSecurityProfile",
        "connect:DescribeTrafficDistributionGroup",
        "connect:DescribeUser",
        "connect:DescribeView",
        "connect:GetTaskTemplate",
        "connect:ListApprovedOrigins",
        "connect:ListEvaluationForms",
        "connect:ListInstanceAttributes",
        "connect:ListInstances",
        "connect:ListInstanceStorageConfigs",
        "connect:ListIntegrationAssociations",
        "connect:ListPhoneNumbers",
        "connect:ListPhoneNumbersV2",
        "connect:ListPredefinedAttributes",
        "connect:ListPrompts",
        "connect:ListQueueQuickConnects",
        "connect:ListQueues",
        "connect:ListQuickConnects",
        "connect:ListRoutingProfileQueues",
        "connect:ListRoutingProfiles",
        "connect:ListRules",
        "connect:ListSecurityKeys",
        "connect:ListSecurityProfileApplications",
        "connect:ListSecurityProfilePermissions",
        "connect:ListSecurityProfiles",
        "connect:ListTagsForResource",
        "connect:ListTaskTemplates",
        "connect:ListTrafficDistributionGroups",
        "connect:ListUsers",
        "connect:ListViewVersions",
        "connect:ListViews",
        "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",
        "datazone:GetDomain",
        "datazone:ListDomains",
        "dax:DescribeClusters",
        "dax:DescribeParameterGroups",
        "dax:DescribeParameters",
        "dax:DescribeSubnetGroups",
        "dax:ListTags",
        "deadline:GetFarm",
        "deadline:GetFleet",
        "deadline:GetMonitor",
        "deadline:GetQueueFleetAssociation",
        "deadline:ListFarms",
        "deadline:ListFleets",
        "deadline:ListMonitors",
        "deadline:ListQueueFleetAssociations",
        "deadline:ListTagsForResource",
        "detective:ListGraphs",
        "detective:ListOrganizationAdminAccount",
        "detective:ListTagsForResource",
```

```
        "devicefarm:GetInstanceProfile",
        "devicefarm:GetNetworkProfile",
        "devicefarm:GetProject",
        "devicefarm:GetTestGridProject",
        "devicefarm:ListInstanceProfiles",
        "devicefarm:ListNetworkProfiles",
        "devicefarm:ListProjects",
        "devicefarm:ListTagsForResource",
        "devicefarm:ListTestGridProjects",
        "devops-guru:GetResourceCollection",
        "devops-guru:ListNotificationChannels",
        "directconnect:DescribeConnections",
        "dms:DescribeCertificates",
        "dms:DescribeDataMigrations",
        "dms:DescribeEndpoints",
        "dms:DescribeEventSubscriptions",
        "dms:DescribeReplicationConfigs",
        "dms:DescribeReplicationInstances",
        "dms:DescribeReplicationSubnetGroups",
        "dms:DescribeReplicationTaskAssessmentRuns",
        "dms:DescribeReplicationTasks",
        "dms:ListMigrationProjects",
        "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:GetAllowedImagesSettings",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetInstanceTypesFromInstanceRequirements",
        "ec2:GetIpamPoolAllocations",
        "ec2:GetIpamPoolCidrs",
        "ec2:GetManagedPrefixListEntries",
```

```
        "ec2:GetNetworkInsightsAccessScopeAnalysisFindings",
        "ec2:GetNetworkInsightsAccessScopeContent",
        "ec2:GetSnapshotBlockPublicAccessState",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:GetVerifiedAccessGroupPolicy",
        "ec2:SearchLocalGatewayRoutes",
        "ec2:SearchTransitGatewayMulticastGroups",
        "ecr-public:DescribeRepositories",
        "ecr-public:GetRepositoryCatalogData",
        "ecr-public:GetRepositoryPolicy",
        "ecr-public:ListTagsForResource",
        "ecr:BatchGetRepositoryScanningConfiguration",
        "ecr:DescribePullThroughCacheRules",
        "ecr:DescribeRegistry",
        "ecr:DescribeRepositories",
        "ecr:DescribeRepositoryCreationTemplates",
        "ecr:GetLifecyclePolicy",
        "ecr:GetRegistryPolicy",
        "ecr:GetRepositoryPolicy",
        "ecr:ListTagsForResource",
        "ecs:DescribeCapacityProviders",
        "ecs:DescribeClusters",
        "ecs:DescribeServices",
        "ecs:DescribeTaskDefinition",
        "ecs:DescribeTaskSets",
        "ecs:ListClusters",
        "ecs:ListServices",
        "ecs:ListTagsForResource",
        "ecs:ListTaskDefinitionFamilies",
        "ecs:ListTaskDefinitions",
        "eks:DescribeAccessEntry",
        "eks:DescribeAddon",
        "eks:DescribeCluster",
        "eks:DescribeFargateProfile",
        "eks:DescribeIdentityProviderConfig",
        "eks:DescribeNodegroup",
        "eks:DescribePodIdentityAssociation",
        "eks:ListAccessEntries",
        "eks:ListAddons",
        "eks:ListAssociatedAccessPolicies",
        "eks:ListClusters",
        "eks:ListFargateProfiles",
        "eks:ListIdentityProviderConfigs",
        "eks:ListNodegroups",
```

```
        "eks:ListPodIdentityAssociations",
        "eks:ListTagsForResource",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeCacheParameterGroups",
        "elasticache:DescribeCacheParameters",
        "elasticache:DescribeCacheSecurityGroups",
        "elasticache:DescribeCacheSubnetGroups",
        "elasticache:DescribeGlobalReplicationGroups",
        "elasticache:DescribeReplicationGroups",
        "elasticache:DescribeSnapshots",
        "elasticache:DescribeUserGroups",
        "elasticache:DescribeUsers",
        "elasticache:ListTagsForResource",
        "elasticbeanstalk:DescribeConfigurationSettings",
        "elasticbeanstalk:DescribeEnvironments",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeBackupPolicy",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeMountTargetSecurityGroups",
        "elasticfilesystem:DescribeTags",
        "elasticloadbalancing:DescribeListenerCertificates",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancerPolicies",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:DescribeSecurityConfiguration",
        "elasticmapreduce:DescribeStep",
        "elasticmapreduce:DescribeStudio",
        "elasticmapreduce:GetAutoTerminationPolicy",
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:GetManagedScalingPolicy",
        "elasticmapreduce:GetStudioSessionMapping",
        "elasticmapreduce:ListBootstrapActions",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListInstanceFleets",
```

```
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListSecurityConfigurations",
        "elasticmapreduce:ListSteps",
        "elasticmapreduce:ListStudios",
        "elasticmapreduce:ListStudioSessionMappings",
        "emr-containers:DescribeJobRun",
        "emr-containers:DescribeVirtualCluster",
        "emr-containers:ListJobRuns",
        "emr-containers:ListManagedEndpoints",
        "emr-containers:ListVirtualClusters",
        "emr-serverless:GetApplication",
        "emr-serverless:GetJobRun",
        "emr-serverless:ListApplications",
        "emr-serverless:ListJobRuns",
        "entityresolution:GetIdMappingWorkflow",
        "entityresolution:GetMatchingWorkflow",
        "entityresolution:GetSchemaMapping",
        "entityresolution:ListIdMappingWorkflows",
        "entityresolution:ListMatchingWorkflows",
        "entityresolution:ListSchemaMappings",
        "entityresolution:ListTagsForResource",
        "es:DescribeDomain",
        "es:DescribeDomains",
        "es:DescribeElasticsearchDomain",
        "es:DescribeElasticsearchDomains",
        "es:GetCompatibleElasticsearchVersions",
        "es:GetCompatibleVersions",
        "es:ListDomainNames",
        "es:ListTags",
        "events:DescribeApiDestination",
        "events:DescribeArchive",
        "events:DescribeConnection",
        "events:DescribeEndpoint",
        "events:DescribeEventBus",
        "events:DescribeRule",
        "events:ListApiDestinations",
        "events:ListArchives",
        "events:ListConnections",
        "events:ListEndpoints",
        "events:ListEventBuses",
        "events:ListRules",
        "events:ListTagsForResource",
        "events:ListTargetsByRule",
```

```
        "evidently:GetLaunch",
        "evidently:GetProject",
        "evidently:GetSegment",
        "evidently:ListLaunches",
        "evidently:ListProjects",
        "evidently:ListSegments",
        "evidently:ListTagsForResource",
        "finspace:GetEnvironment",
        "finspace:ListEnvironments",
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams",
        "firehose:ListTagsForDeliveryStream",
        "fis:GetExperimentTemplate",
        "fis: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:DescribeContainerGroupDefinition",
```

```
        "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:ListContainerGroupDefinitions",
        "gamelift:ListFleets",
        "gamelift:ListGameServerGroups",
        "gamelift:ListScripts",
        "gamelift:ListTagsForResource",
        "geo:DescribeGeofenceCollection",
        "geo:DescribeKey",
        "geo:DescribeMap",
        "geo:DescribePlaceIndex",
        "geo:DescribeRouteCalculator",
        "geo:DescribeTracker",
        "geo:ListGeofenceCollections",
        "geo:ListKeys",
        "geo:ListMaps",
        "geo:ListPlaceIndexes",
        "geo:ListRouteCalculators",
        "geo:ListTrackerConsumers",
        "geo:ListTrackers",
        "globalaccelerator:DescribeAccelerator",
        "globalaccelerator:DescribeCrossAccountAttachment",
        "globalaccelerator:DescribeEndpointGroup",
        "globalaccelerator:DescribeListener",
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListCrossAccountAttachments",
        "globalaccelerator:ListEndpointGroups",
        "globalaccelerator:ListListeners",
        "globalaccelerator:ListTagsForResource",
        "glue:BatchGetDevEndpoints",
        "glue:BatchGetJobs",
```

```
        "glue:BatchGetWorkflows",
        "glue:GetClassifier",
        "glue:GetClassifiers",
        "glue:GetCrawler",
        "glue:GetCrawlers",
        "glue:GetDataCatalogEncryptionSettings",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetDevEndpoint",
        "glue:GetDevEndpoints",
        "glue:GetJob",
        "glue:GetJobs",
        "glue:GetMLTransform",
        "glue:GetMLTransforms",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetRegistry",
        "glue:GetSecurityConfiguration",
        "glue:GetSecurityConfigurations",
        "glue:GetTable",
        "glue:GetTags",
        "glue:GetTrigger",
        "glue:GetWorkflow",
        "glue:ListCrawlers",
        "glue:ListDevEndpoints",
        "glue:ListJobs",
        "glue:ListMLTransforms",
        "glue:ListRegistries",
        "glue:ListTriggers",
        "glue:ListWorkflows",
        "grafana:DescribeWorkspace",
        "grafana:DescribeWorkspaceAuthentication",
        "grafana:DescribeWorkspaceConfiguration",
        "grafana:ListWorkspaces",
        "greengrass:DescribeComponent",
        "greengrass:GetComponent",
        "greengrass: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:GetMalwareProtectionPlan",
        "guardduty:GetMasterAccount",
        "guardduty:GetMemberDetectors",
        "guardduty:GetMembers",
        "guardduty:GetThreatIntelSet",
        "guardduty:ListDetectors",
        "guardduty:ListFilters",
        "guardduty:ListFindings",
        "guardduty:ListIPSets",
        "guardduty:ListMalwareProtectionPlans",
        "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:ListPolicies",
        "iam:ListPolicyVersions",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListSAMLProviders",
        "iam:ListServerCertificates",
        "iam:ListUserPolicies",
        "iam:ListUsers",
        "iam:ListVirtualMFADevices",
        "identitystore:DescribeGroup",
        "identitystore:DescribeGroupMembership",
        "identitystore:ListGroupMemberships",
        "identitystore:ListGroupMembershipsForMember",
        "identitystore:ListGroups",
        "imagebuilder:GetComponent",
        "imagebuilder:GetContainerRecipe",
        "imagebuilder:GetDistributionConfiguration",
        "imagebuilder:GetImage",
        "imagebuilder:GetImagePipeline",
        "imagebuilder:GetImageRecipe",
        "imagebuilder:GetInfrastructureConfiguration",
        "imagebuilder:GetLifecyclePolicy",
        "imagebuilder:ListComponentBuildVersions",
        "imagebuilder:ListComponents",
        "imagebuilder:ListContainerRecipes",
        "imagebuilder:ListDistributionConfigurations",
        "imagebuilder:ListImageBuildVersions",
        "imagebuilder:ListImagePipelines",
        "imagebuilder:ListImageRecipes",
        "imagebuilder:ListImages",
        "imagebuilder:ListInfrastructureConfigurations",
        "imagebuilder:ListLifecyclePolicies",
```

```
        "inspector2:BatchGetAccountStatus",
        "inspector2:GetDelegatedAdminAccount",
        "inspector2:ListFilters",
        "inspector2:ListMembers",
        "internetmonitor:GetMonitor",
        "internetmonitor:ListMonitors",
        "internetmonitor:ListTagsForResource",
        "iot:DescribeAccountAuditConfiguration",
        "iot:DescribeAuthorizer",
        "iot:DescribeBillingGroup",
        "iot:DescribeCACertificate",
        "iot:DescribeCertificate",
        "iot:DescribeCertificateProvider",
        "iot:DescribeCustomMetric",
        "iot:DescribeDimension",
        "iot:DescribeDomainConfiguration",
        "iot:DescribeFleetMetric",
        "iot:DescribeJobTemplate",
        "iot:DescribeMitigationAction",
        "iot:DescribeProvisioningTemplate",
        "iot:DescribeRoleAlias",
        "iot:DescribeScheduledAudit",
        "iot:DescribeSecurityProfile",
        "iot:DescribeThingGroup",
        "iot:DescribeThingType",
        "iot:GetPackage",
        "iot:GetPackageVersion",
        "iot:GetPolicy",
        "iot:GetTopicRule",
        "iot:GetTopicRuleDestination",
        "iot:ListAuthorizers",
        "iot:ListBillingGroups",
        "iot:ListCACertificates",
        "iot:ListCertificateProviders",
        "iot:ListCertificates",
        "iot:ListCustomMetrics",
        "iot:ListDimensions",
        "iot:ListDomainConfigurations",
        "iot:ListFleetMetrics",
        "iot:ListJobTemplates",
        "iot:ListMitigationActions",
        "iot:ListPackageVersions",
        "iot:ListPackages",
        "iot:ListPolicies",
```

```
        "iot:ListProvisioningTemplates",
        "iot:ListRoleAliases",
        "iot:ListScheduledAudits",
        "iot:ListSecurityProfiles",
        "iot:ListSecurityProfilesForTarget",
        "iot:ListTagsForResource",
        "iot:ListTargetsForSecurityProfile",
        "iot:ListThingGroups",
        "iot:ListThingTypes",
        "iot:ListTopicRuleDestinations",
        "iot:ListTopicRules",
        "iot:ListV2LoggingLevels",
        "iot:ValidateSecurityProfileBehaviors",
        "iotanalytics:DescribeChannel",
        "iotanalytics:DescribeDataset",
        "iotanalytics:DescribeDatastore",
        "iotanalytics:DescribePipeline",
        "iotanalytics:ListChannels",
        "iotanalytics:ListDatasets",
        "iotanalytics:ListDatastores",
        "iotanalytics:ListPipelines",
        "iotanalytics:ListTagsForResource",
        "iotdeviceadvisor:GetSuiteDefinition",
        "iotdeviceadvisor:ListSuiteDefinitions",
        "iotevents:DescribeAlarmModel",
        "iotevents:DescribeDetectorModel",
        "iotevents:DescribeInput",
        "iotevents:ListAlarmModels",
        "iotevents:ListDetectorModels",
        "iotevents:ListInputs",
        "iotevents:ListTagsForResource",
        "iotfleetwise:GetDecoderManifest",
        "iotfleetwise:GetFleet",
        "iotfleetwise:GetModelManifest",
        "iotfleetwise:GetSignalCatalog",
        "iotfleetwise:GetVehicle",
        "iotfleetwise:ListDecoderManifestNetworkInterfaces",
        "iotfleetwise:ListDecoderManifests",
        "iotfleetwise:ListDecoderManifestSignals",
        "iotfleetwise:ListFleets",
        "iotfleetwise:ListModelManifestNodes",
        "iotfleetwise:ListModelManifests",
        "iotfleetwise:ListSignalCatalogNodes",
        "iotfleetwise:ListSignalCatalogs",
```

```
        "iotfleetwise:ListTagsForResource",
        "iotfleetwise:ListVehicles",
        "iotsitewise:DescribeAccessPolicy",
        "iotsitewise:DescribeAsset",
        "iotsitewise:DescribeAssetModel",
        "iotsitewise:DescribeDashboard",
        "iotsitewise:DescribeGateway",
        "iotsitewise:DescribePortal",
        "iotsitewise:DescribeProject",
        "iotsitewise:ListAccessPolicies",
        "iotsitewise:ListAssetModelCompositeModels",
        "iotsitewise:ListAssetModelProperties",
        "iotsitewise:ListAssetModels",
        "iotsitewise:ListAssetProperties",
        "iotsitewise:ListAssets",
        "iotsitewise:ListAssociatedAssets",
        "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:GetDestination",
        "iotwireless:GetDeviceProfile",
        "iotwireless:GetFuotaTask",
        "iotwireless:GetMulticastGroup",
        "iotwireless:GetNetworkAnalyzerConfiguration",
        "iotwireless:GetServiceProfile",
        "iotwireless:GetWirelessDevice",
        "iotwireless:GetWirelessGateway",
        "iotwireless:GetWirelessGatewayTaskDefinition",
        "iotwireless:ListDestinations",
        "iotwireless:ListDeviceProfiles",
```

```
        "iotwireless:ListFuotaTasks",
        "iotwireless:ListMulticastGroups",
        "iotwireless:ListNetworkAnalyzerConfigurations",
        "iotwireless:ListServiceProfiles",
        "iotwireless:ListTagsForResource",
        "iotwireless:ListWirelessDevices",
        "iotwireless:ListWirelessGateways",
        "iotwireless:ListWirelessGatewayTaskDefinitions",
        "ivs:GetChannel",
        "ivs:GetEncoderConfiguration",
        "ivs:GetPlaybackKeyPair",
        "ivs:GetPlaybackRestrictionPolicy",
        "ivs:GetRecordingConfiguration",
        "ivs:GetStage",
        "ivs:GetStorageConfiguration",
        "ivs:GetStreamKey",
        "ivs:ListChannels",
        "ivs:ListEncoderConfigurations",
        "ivs:ListPlaybackKeyPairs",
        "ivs:ListPlaybackRestrictionPolicies",
        "ivs:ListPublicKeys",
        "ivs:ListRecordingConfigurations",
        "ivs:ListStages",
        "ivs:ListStorageConfigurations",
        "ivs:ListStreamKeys",
        "ivs:ListTagsForResource",
        "ivschat:GetLoggingConfiguration",
        "ivschat:GetRoom",
        "ivschat:ListLoggingConfigurations",
        "ivschat:ListRooms",
        "ivschat:ListTagsForResource",
        "kafka:DescribeCluster",
        "kafka:DescribeClusterV2",
        "kafka:DescribeConfiguration",
        "kafka:DescribeConfigurationRevision",
        "kafka:DescribeVpcConnection",
        "kafka:GetClusterPolicy",
        "kafka:ListClusters",
        "kafka:ListClustersV2",
        "kafka:ListConfigurations",
        "kafka:ListScramSecrets",
        "kafka:ListTagsForResource",
        "kafka:ListVpcConnections",
        "kafkaconnect:DescribeConnector",
```

```
        "kafkaconnect:DescribeCustomPlugin",
        "kafkaconnect:DescribeWorkerConfiguration",
        "kafkaconnect:ListConnectors",
        "kafkaconnect:ListCustomPlugins",
        "kafkaconnect:ListTagsForResource",
        "kafkaconnect:ListWorkerConfigurations",
        "kendra:DescribeIndex",
        "kendra:ListIndices",
        "kendra:ListTagsForResource",
        "kinesis:DescribeStreamConsumer",
        "kinesis:DescribeStreamSummary",
        "kinesis:GetResourcePolicy",
        "kinesis:ListStreamConsumers",
        "kinesis:ListStreams",
        "kinesis:ListTagsForStream",
        "kinesisanalytics:DescribeApplication",
        "kinesisanalytics:ListApplications",
        "kinesisanalytics:ListTagsForResource",
        "kinesisvideo:DescribeSignalingChannel",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:ListSignalingChannels",
        "kinesisvideo:ListStreams",
        "kinesisvideo:ListTagsForResource",
        "kinesisvideo:ListTagsForStream",
        "kms:DescribeKey",
        "kms:GetKeyPolicy",
        "kms:GetKeyRotationStatus",
        "kms:ListAliases",
        "kms:ListKeys",
        "kms:ListResourceTags",
        "lakeformation:DescribeLakeFormationIdentityCenterConfiguration",
        "lakeformation:DescribeResource",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:ListDataCellsFilter",
        "lakeformation:ListPermissions",
        "lakeformation:ListResources",
        "lambda:GetAlias",
        "lambda:GetCodeSigningConfig",
        "lambda:GetEventSourceMapping",
        "lambda:GetFunction",
        "lambda:GetFunctionCodeSigningConfig",
        "lambda:GetFunctionConfiguration",
        "lambda:GetFunctionUrlConfig",
        "lambda:GetLayerVersion",
```

```
        "lambda:GetPolicy",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:GetRuntimeManagementConfig",
        "lambda:ListAliases",
        "lambda:ListCodeSigningConfigs",
        "lambda:ListEventSourceMappings",
        "lambda:ListFunctionEventInvokeConfigs",
        "lambda:ListFunctionUrlConfigs",
        "lambda:ListFunctions",
        "lambda:ListLayers",
        "lambda:ListLayerVersions",
        "lambda:ListTags",
        "lambda:ListVersionsByFunction",
        "launchwizard:GetDeployment",
        "launchwizard:ListDeploymentEvents",
        "launchwizard:ListDeployments",
        "launchwizard:ListTagsForResource",
        "lex:DescribeBot",
        "lex:DescribeBotAlias",
        "lex:DescribeBotVersion",
        "lex:DescribeResourcePolicy",
        "lex:ListBotAliases",
        "lex:ListBotLocales",
        "lex:ListBots",
        "lex:ListBotVersions",
        "lex:ListTagsForResource",
        "license-manager:GetGrant",
        "license-manager:GetLicense",
        "license-manager:ListDistributedGrants",
        "license-manager:ListLicenses",
        "license-manager:ListReceivedGrants",
        "lightsail:GetActiveNames",
        "lightsail:GetAlarms",
        "lightsail:GetBuckets",
        "lightsail:GetCertificates",
        "lightsail:GetContainerServices",
        "lightsail:GetDisk",
        "lightsail:GetDisks",
        "lightsail:GetDistributions",
        "lightsail:GetDomain",
        "lightsail:GetDomains",
        "lightsail:GetInstance",
        "lightsail:GetInstanceSnapshot",
        "lightsail:GetInstanceSnapshots",
```

```
        "lightsail:GetInstances",
        "lightsail:GetKeyPair",
        "lightsail:GetLoadBalancer",
        "lightsail:GetLoadBalancers",
        "lightsail:GetLoadBalancerTlsCertificates",
        "lightsail:GetOperations",
        "lightsail:GetRelationalDatabase",
        "lightsail:GetRelationalDatabaseParameters",
        "lightsail:GetRelationalDatabases",
        "lightsail:GetStaticIp",
        "lightsail:GetStaticIps",
        "logs:DescribeAccountPolicies",
        "logs:DescribeDeliveries",
        "logs:DescribeDeliveryDestinations",
        "logs:DescribeDeliverySources",
        "logs:DescribeDestinations",
        "logs:DescribeIndexPolicies",
        "logs:DescribeLogGroups",
        "logs:DescribeMetricFilters",
        "logs:DescribeResourcePolicies",
        "logs:GetDataProtectionPolicy",
        "logs:GetDelivery",
        "logs:GetDeliveryDestination",
        "logs:GetDeliveryDestinationPolicy",
        "logs:GetDeliverySource",
        "logs:GetLogAnomalyDetector",
        "logs:GetLogDelivery",
        "logs:ListLogAnomalyDetectors",
        "logs:ListLogDeliveries",
        "logs:ListTagsForResource",
        "logs:ListTagsLogGroup",
        "lookoutequipment:DescribeInferenceScheduler",
        "lookoutequipment:ListTagsForResource",
        "lookoutmetrics:DescribeAlert",
        "lookoutmetrics:DescribeAnomalyDetector",
        "lookoutmetrics:ListAlerts",
        "lookoutmetrics:ListAnomalyDetectors",
        "lookoutmetrics:ListMetricSets",
        "lookoutmetrics:ListTagsForResource",
        "lookoutvision:DescribeProject",
        "lookoutvision:ListProjects",
        "m2:GetEnvironment",
        "m2:ListEnvironments",
        "m2:ListTagsForResource",
```

```
        "macie2:DescribeOrganizationConfiguration",
        "macie2:GetAllowList",
        "macie2:GetAutomatedDiscoveryConfiguration",
        "macie2:GetClassificationExportConfiguration",
        "macie2:GetCustomDataIdentifier",
        "macie2:GetFindingsPublicationConfiguration",
        "macie2:GetMacieSession",
        "macie2:ListAllowLists",
        "macie2:ListAutomatedDiscoveryAccounts",
        "macie2:ListCustomDataIdentifiers",
        "macie2:ListTagsForResource",
        "managedblockchain:GetAccessor",
        "managedblockchain:GetMember",
        "managedblockchain:GetNetwork",
        "managedblockchain:GetNode",
        "managedblockchain:ListAccessors",
        "managedblockchain:ListInvitations",
        "managedblockchain:ListMembers",
        "managedblockchain:ListNodes",
        "mediaconnect:DescribeBridge",
        "mediaconnect:DescribeFlow",
        "mediaconnect:DescribeGateway",
        "mediaconnect:ListBridges",
        "mediaconnect:ListFlows",
        "mediaconnect:ListGateways",
        "mediaconnect:ListTagsForResource",
        "medialive:DescribeChannelPlacementGroup",
        "medialive:DescribeMultiplexProgram",
        "medialive:ListChannelPlacementGroups",
        "medialive:ListMultiplexPrograms",
        "medialive:ListMultiplexes",
        "medialive:ListTagsForResource",
        "mediapackage-vod:DescribeAsset",
        "mediapackage-vod:DescribePackagingConfiguration",
        "mediapackage-vod:DescribePackagingGroup",
        "mediapackage-vod:ListAssets",
        "mediapackage-vod:ListPackagingConfigurations",
        "mediapackage-vod:ListPackagingGroups",
        "mediapackage-vod:ListTagsForResource",
        "mediapackagev2:GetChannel",
        "mediapackagev2:GetChannelGroup",
        "mediapackagev2:GetOriginEndpoint",
        "mediapackagev2:ListChannelGroups",
        "mediapackagev2:ListChannels",
```

```
        "mediapackagev2:ListOriginEndpoints",
        "mediatailor:DescribeChannel",
        "mediatailor:DescribeLiveSource",
        "mediatailor:DescribeSourceLocation",
        "mediatailor:DescribeVodSource",
        "mediatailor:GetPlaybackConfiguration",
        "mediatailor:ListChannels",
        "mediatailor:ListLiveSources",
        "mediatailor:ListPlaybackConfigurations",
        "mediatailor:ListSourceLocations",
        "mediatailor:ListVodSources",
        "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:GetTransitGatewayPeering",
        "networkmanager:GetTransitGatewayRegistrations",
```

```
        "networkmanager:ListConnectPeers",
        "networkmanager:ListPeerings",
        "networkmanager:ListTagsForResource",
        "nimble:GetLaunchProfile",
        "nimble:GetLaunchProfileDetails",
        "nimble:GetStreamingImage",
        "nimble:GetStudio",
        "nimble:GetStudioComponent",
        "nimble:ListLaunchProfiles",
        "nimble:ListStreamingImages",
        "nimble:ListStudioComponents",
        "nimble:ListStudios",
        "oam:GetSink",
        "oam:GetSinkPolicy",
        "oam:ListSinks",
        "omics:GetAnnotationStore",
        "omics:GetRunGroup",
        "omics:GetSequenceStore",
        "omics:GetVariantStore",
        "omics:GetWorkflow",
        "omics:ListAnnotationStores",
        "omics:ListRunGroups",
        "omics:ListSequenceStores",
        "omics:ListTagsForResource",
        "omics:ListVariantStores",
        "omics:ListWorkflows",
        "opsworks:DescribeInstances",
        "opsworks:DescribeLayers",
        "opsworks:DescribeTimeBasedAutoScaling",
        "opsworks:DescribeVolumes",
        "opsworks:ListTags",
        "organizations:DescribeAccount",
        "organizations:DescribeEffectivePolicy",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribePolicy",
        "organizations:DescribeResourcePolicy",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListPolicies",
```

```
        "organizations:ListPoliciesForTarget",
        "organizations:ListRoots",
        "organizations:ListTagsForResource",
        "organizations:ListTargetsForPolicy",
        "osis:GetPipeline",
        "osis:ListPipelines",
        "osis:ListTagsForResource",
        "panorama:DescribeApplicationInstance",
        "panorama:DescribeApplicationInstanceDetails",
        "panorama:DescribePackage",
        "panorama:DescribePackageVersion",
        "panorama:ListApplicationInstances",
        "panorama:ListNodes",
        "panorama:ListPackages",
        "payment-cryptography:GetAlias",
        "payment-cryptography:GetKey",
        "payment-cryptography:ListAliases",
        "payment-cryptography:ListKeys",
        "payment-cryptography:ListTagsForResource",
        "pca-connector-ad:GetConnector",
        "pca-connector-ad:GetDirectoryRegistration",
        "pca-connector-ad:ListConnectors",
        "pca-connector-ad:ListDirectoryRegistrations",
        "pca-connector-ad:ListTagsForResource",
        "pca-connector-scep:GetConnector",
        "pca-connector-scep:ListConnectors",
        "pca-connector-scep:ListTagsForResource",
        "personalize:DescribeDataset",
        "personalize:DescribeDatasetGroup",
        "personalize:DescribeSchema",
        "personalize:DescribeSolution",
        "personalize:ListDatasetGroups",
        "personalize:ListDatasetImportJobs",
        "personalize:ListDatasets",
        "personalize:ListSchemas",
        "personalize:ListSolutions",
        "personalize:ListTagsForResource",
        "pipes:DescribePipe",
        "pipes:ListPipes",
        "profile:GetDomain",
        "profile:GetIntegration",
        "profile:GetProfileObjectType",
        "profile:ListDomains",
        "profile:ListIntegrations",
```

```
        "profile:ListProfileObjectTypes",
        "profile:ListTagsForResource",
        "qbusiness:GetApplication",
        "qbusiness:ListApplications",
        "qbusiness:ListTagsForResource",
        "quicksight:DescribeAccountSubscription",
        "quicksight:DescribeAnalysis",
        "quicksight:DescribeAnalysisPermissions",
        "quicksight:DescribeDashboard",
        "quicksight:DescribeDashboardPermissions",
        "quicksight:DescribeDataSet",
        "quicksight:DescribeDataSetPermissions",
        "quicksight:DescribeDataSetRefreshProperties",
        "quicksight:DescribeDataSource",
        "quicksight:DescribeDataSourcePermissions",
        "quicksight:DescribeRefreshSchedule",
        "quicksight:DescribeTemplate",
        "quicksight:DescribeTemplatePermissions",
        "quicksight:DescribeTheme",
        "quicksight:DescribeThemePermissions",
        "quicksight:DescribeTopic",
        "quicksight:ListAnalyses",
        "quicksight:ListDashboards",
        "quicksight:ListDataSets",
        "quicksight:ListDataSources",
        "quicksight:ListRefreshSchedules",
        "quicksight:ListTagsForResource",
        "quicksight:ListTemplates",
        "quicksight:ListThemes",
        "quicksight:ListTopics",
        "ram:GetPermission",
        "ram:GetResourceShareAssociations",
        "ram:GetResourceShares",
        "ram:ListPermissionAssociations",
        "ram:ListPermissions",
        "ram:ListPermissionVersions",
        "ram:ListResources",
        "ram:ListResourceSharePermissions",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBEngineVersions",
```

```
        "rds:DescribeDBInstances",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBProxies",
        "rds:DescribeDBProxyEndpoints",
        "rds:DescribeDBProxyTargetGroups",
        "rds:DescribeDBProxyTargets",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBShardGroups",
        "rds:DescribeDBSnapshotAttributes",
        "rds:DescribeDBSnapshots",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultClusterParameters",
        "rds:DescribeEngineDefaultParameters",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeGlobalClusters",
        "rds:DescribeIntegrations",
        "rds:DescribeOptionGroups",
        "rds:ListTagsForResource",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListSnapshotCopyConfigurations",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:ListWorkgroups",
        "redshift:DescribeClusterParameterGroups",
        "redshift:DescribeClusterParameters",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSecurityGroups",
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeClusterSubnetGroups",
        "redshift:DescribeEndpointAccess",
        "redshift:DescribeEndpointAuthorization",
        "redshift:DescribeEventSubscriptions",
        "redshift:DescribeIntegrations",
        "redshift:DescribeLoggingStatus",
        "redshift:DescribeScheduledActions",
        "redshift:DescribeTags",
        "redshift:GetResourcePolicy",
        "refactor-spaces:GetEnvironment",
        "refactor-spaces:GetService",
        "refactor-spaces:ListApplications",
        "refactor-spaces:ListEnvironments",
        "refactor-spaces:ListServices",
```

```
        "refactor-spaces:ListTagsForResource",
        "rekognition:DescribeProjects",
        "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",
        "rolesanywhere:GetCrl",
        "rolesanywhere:GetProfile",
        "rolesanywhere:GetTrustAnchor",
        "rolesanywhere:ListCrls",
        "rolesanywhere:ListProfiles",
        "rolesanywhere:ListTagsForResource",
        "rolesanywhere:ListTrustAnchors",
        "route53-recovery-control-config:DescribeCluster",
        "route53-recovery-control-config:DescribeControlPanel",
        "route53-recovery-control-config:DescribeRoutingControl",
        "route53-recovery-control-config:DescribeSafetyRule",
        "route53-recovery-control-config:ListClusters",
        "route53-recovery-control-config:ListControlPanels",
        "route53-recovery-control-config:ListRoutingControls",
        "route53-recovery-control-config:ListSafetyRules",
        "route53-recovery-control-config:ListTagsForResource",
        "route53-recovery-readiness:GetCell",
        "route53-recovery-readiness:GetReadinessCheck",
        "route53-recovery-readiness:GetRecoveryGroup",
```

```
        "route53-recovery-readiness:GetResourceSet",
        "route53-recovery-readiness:ListCells",
        "route53-recovery-readiness:ListReadinessChecks",
        "route53-recovery-readiness:ListRecoveryGroups",
        "route53-recovery-readiness:ListResourceSets",
        "route53:GetChange",
        "route53:GetDNSSEC",
        "route53:GetHealthCheck",
        "route53:GetHostedZone",
        "route53:ListCidrBlocks",
        "route53:ListCidrCollections",
        "route53:ListCidrLocations",
        "route53:ListHealthChecks",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName",
        "route53:ListQueryLoggingConfigs",
        "route53:ListResourceRecordSets",
        "route53:ListTagsForResource",
        "route53profiles:GetProfile",
        "route53profiles:GetProfileAssociation",
        "route53profiles:ListProfileAssociations",
        "route53profiles:ListProfiles",
        "route53profiles:ListTagsForResource",
        "route53resolver:GetFirewallDomainList",
        "route53resolver:GetFirewallRuleGroup",
        "route53resolver:GetFirewallRuleGroupAssociation",
        "route53resolver: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:GetAccessGrant",
        "s3:GetAccessGrantsInstance",
        "s3:GetAccessGrantsLocation",
        "s3:GetAccessPoint",
        "s3:GetAccessPointForObjectLambda",
        "s3:GetAccessPointPolicy",
        "s3:GetAccessPointPolicyForObjectLambda",
        "s3:GetAccessPointPolicyStatus",
        "s3:GetAccessPointPolicyStatusForObjectLambda",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketAbac",
        "s3:GetBucketCORS",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketNotification",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketRequestPayment",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "s3:GetBucketWebsite",
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetMultiRegionAccessPoint",
        "s3:GetMultiRegionAccessPointPolicy",
        "s3:GetMultiRegionAccessPointPolicyStatus",
```

```
        "s3:GetReplicationConfiguration",
        "s3:GetStorageLensConfiguration",
        "s3:GetStorageLensConfigurationTagging",
        "s3:GetStorageLensGroup",
        "s3:ListAccessGrants",
        "s3:ListAccessGrantsInstances",
        "s3:ListAccessGrantsLocations",
        "s3:ListAccessPoints",
        "s3:ListAccessPointsForObjectLambda",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListMultiRegionAccessPoints",
        "s3:ListStorageLensConfigurations",
        "s3:ListStorageLensGroups",
        "s3:ListTagsForResource",
        "s3express:GetBucketPolicy",
        "s3express:GetEncryptionConfiguration",
        "s3express:GetLifecycleConfiguration",
        "s3express:ListAllMyDirectoryBuckets",
        "s3tables:GetTableBucket",
        "s3tables:GetTableBucketEncryption",
        "s3tables:GetTableBucketMaintenanceConfiguration",
        "s3tables:GetTableBucketPolicy",
        "s3tables:ListTableBuckets",
        "sagemaker:DescribeApp",
        "sagemaker:DescribeAppImageConfig",
        "sagemaker:DescribeCluster",
        "sagemaker:DescribeCodeRepository",
        "sagemaker:DescribeDataQualityJobDefinition",
        "sagemaker:DescribeDeviceFleet",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeFeatureGroup",
        "sagemaker:DescribeImage",
        "sagemaker:DescribeImageVersion",
        "sagemaker:DescribeInferenceComponent",
        "sagemaker:DescribeInferenceExperiment",
        "sagemaker:DescribeMlflowTrackingServer",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeModelBiasJobDefinition",
        "sagemaker:DescribeModelCard",
        "sagemaker:DescribeModelExplainabilityJobDefinition",
        "sagemaker:DescribeModelPackage",
```

```
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribeModelQualityJobDefinition",
        "sagemaker:DescribeMonitoringSchedule",
        "sagemaker:DescribeNotebookInstance",
        "sagemaker:DescribeNotebookInstanceLifecycleConfig",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeProject",
        "sagemaker:DescribeStudioLifecycleConfig",
        "sagemaker:DescribeUserProfile",
        "sagemaker:DescribeWorkteam",
        "sagemaker:GetModelPackageGroupPolicy",
        "sagemaker:ListAppImageConfigs",
        "sagemaker:ListApps",
        "sagemaker:ListClusters",
        "sagemaker:ListCodeRepositories",
        "sagemaker:ListDataQualityJobDefinitions",
        "sagemaker:ListDeviceFleets",
        "sagemaker:ListDomains",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListEndpoints",
        "sagemaker:ListFeatureGroups",
        "sagemaker:ListImages",
        "sagemaker:ListImageVersions",
        "sagemaker:ListInferenceComponents",
        "sagemaker:ListInferenceExperiments",
        "sagemaker:ListMlflowTrackingServers",
        "sagemaker:ListModelBiasJobDefinitions",
        "sagemaker:ListModelCardVersions",
        "sagemaker:ListModelCards",
        "sagemaker:ListModelExplainabilityJobDefinitions",
        "sagemaker:ListModelPackageGroups",
        "sagemaker:ListModelPackages",
        "sagemaker:ListModelQualityJobDefinitions",
        "sagemaker:ListModels",
        "sagemaker:ListMonitoringSchedules",
        "sagemaker:ListNotebookInstanceLifecycleConfigs",
        "sagemaker:ListNotebookInstances",
        "sagemaker:ListPipelines",
        "sagemaker:ListProcessingJobs",
        "sagemaker:ListProjects",
        "sagemaker:ListStudioLifecycleConfigs",
        "sagemaker:ListTags",
        "sagemaker:ListUserProfiles",
```

```
            "sagemaker:ListWorkteams",
            "scheduler:GetSchedule",
            "scheduler:GetScheduleGroup",
            "scheduler:ListScheduleGroups",
            "scheduler:ListSchedules",
            "scheduler:ListTagsForResource",
            "schemas:DescribeDiscoverer",
            "schemas:DescribeRegistry",
            "schemas:DescribeSchema",
            "schemas:GetResourcePolicy",
            "schemas:ListDiscoverers",
            "schemas:ListRegistries",
            "schemas:ListSchemas",
            "sdb:GetAttributes",
            "sdb:ListDomains",
            "secretsmanager:DescribeSecret",
            "secretsmanager:GetResourcePolicy",
            "secretsmanager:ListSecrets",
            "secretsmanager:ListSecretVersionIds",
            "securityhub:DescribeHub",
            "securityhub:DescribeStandardsControls",
            "securityhub:GetEnabledStandards",
            "securitylake:GetSubscriber",
            "securitylake:ListDataLakeExceptions",
            "securitylake:ListDataLakes",
            "securitylake:ListLogSources",
            "securitylake:ListSubscribers",
            "securitylake:ListTagsForResource",
            "serviceCatalog:DescribePortfolioShares",
            "servicecatalog:DescribeServiceAction",
            "servicecatalog:GetAttributeGroup",
            "servicecatalog:ListApplications",
            "servicecatalog:ListAssociatedResources",
            "servicecatalog:ListAttributeGroups",
            "servicecatalog:ListServiceActions",
            "servicecatalog:ListServiceActionsForProvisioningArtifact",
            "servicediscovery:GetInstance",
            "servicediscovery:GetNamespace",
            "servicediscovery:GetService",
            "servicediscovery:ListInstances",
            "servicediscovery:ListNamespaces",
            "servicediscovery:ListServices",
            "servicediscovery:ListTagsForResource",
            "ses:DescribeReceiptRule",
```

```
        "ses:DescribeReceiptRuleSet",
        "ses:GetConfigurationSet",
        "ses:GetConfigurationSetEventDestinations",
        "ses:GetContactList",
        "ses:GetDedicatedIpPool",
        "ses:GetDedicatedIps",
        "ses:GetEmailTemplate",
        "ses:GetTemplate",
        "ses:GetTrafficPolicy",
        "ses:ListConfigurationSets",
        "ses:ListContactLists",
        "ses:ListDedicatedIpPools",
        "ses:ListEmailTemplates",
        "ses:ListReceiptFilters",
        "ses:ListReceiptRuleSets",
        "ses:ListTagsForResource",
        "ses:ListTemplates",
        "ses:ListTrafficPolicies",
        "shield:DescribeDRTAccess",
        "shield:DescribeProtection",
        "shield:DescribeProtectionGroup",
        "shield:DescribeSubscription",
        "shield:ListProtectionGroups",
        "shield:ListTagsForResource",
        "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-contacts:GetContact",
        "ssm-contacts:GetContactChannel",
        "ssm-contacts:ListContactChannels",
        "ssm-contacts:ListContacts",
        "ssm-contacts:ListTagsForResource",
        "ssm-incidents:GetReplicationSet",
```

```
            "ssm-incidents:GetResponsePlan",
            "ssm-incidents:ListReplicationSets",
            "ssm-incidents:ListResponsePlans",
            "ssm-incidents:ListTagsForResource",
            "ssm-quicksetup:GetConfigurationManager",
            "ssm-quicksetup:ListConfigurationManagers",
            "ssm-sap:ListTagsForResource",
            "ssm:DescribeAssociation",
            "ssm:DescribeAutomationExecutions",
            "ssm:DescribeDocument",
            "ssm:DescribeDocumentPermission",
            "ssm:DescribeInstanceInformation",
            "ssm:DescribeMaintenanceWindows",
            "ssm:DescribeParameters",
            "ssm:DescribePatchBaselines",
            "ssm:GetAutomationExecution",
            "ssm:GetDefaultPatchBaseline",
            "ssm:GetDocument",
            "ssm:GetPatchBaseline",
            "ssm:GetResourcePolicies",
            "ssm:GetServiceSetting",
            "ssm:ListAssociations",
            "ssm:ListDocuments",
            "ssm:ListResourceDataSync",
            "ssm:ListTagsForResource",
            "sso:DescribeInstanceAccessControlAttributeConfiguration",
            "sso:DescribePermissionSet",
            "sso:GetInlinePolicyForPermissionSet",
            "sso:ListManagedPoliciesInPermissionSet",
            "sso:ListPermissionSets",
            "sso:ListTagsForResource",
            "states:DescribeActivity",
            "states:DescribeStateMachine",
            "states:DescribeStateMachineAlias",
            "states:ListActivities",
            "states:ListStateMachineAliases",
            "states:ListStateMachines",
            "states:ListTagsForResource",
            "storagegateway:ListGateways",
            "storagegateway:ListTagsForResource",
            "storagegateway:ListVolumes",
            "sts:GetCallerIdentity",
            "support:DescribeCases",
            "synthetics:DescribeCanaries",
```

```
        "synthetics:DescribeCanariesLastRun",
        "synthetics:DescribeRuntimeVersions",
        "synthetics:GetCanary",
        "synthetics:GetCanaryRuns",
        "synthetics:GetGroup",
        "synthetics:ListAssociatedGroups",
        "synthetics:ListGroupResources",
        "synthetics:ListGroups",
        "synthetics:ListTagsForResource",
        "tag:GetResources",
        "timestream:DescribeDatabase",
        "timestream:DescribeEndpoints",
        "timestream:DescribeTable",
        "timestream:ListDatabases",
        "timestream:ListTables",
        "timestream:ListTagsForResource",
        "transfer:DescribeAgreement",
        "transfer:DescribeCertificate",
        "transfer:DescribeConnector",
        "transfer:DescribeProfile",
        "transfer:DescribeServer",
        "transfer:DescribeUser",
        "transfer:DescribeWorkflow",
        "transfer:ListAgreements",
        "transfer:ListCertificates",
        "transfer:ListConnectors",
        "transfer:ListProfiles",
        "transfer:ListServers",
        "transfer:ListTagsForResource",
        "transfer:ListUsers",
        "transfer:ListWorkflows",
        "verifiedpermissions:GetPolicyStore",
        "verifiedpermissions:GetPolicyTemplate",
        "verifiedpermissions:GetSchema",
        "verifiedpermissions:ListPolicyStores",
        "verifiedpermissions:ListPolicyTemplates",
        "verifiedpermissions:ListTagsForResource",
        "voiceid:DescribeDomain",
        "voiceid:ListTagsForResource",
        "vpc-lattice:GetAccessLogSubscription",
        "vpc-lattice:GetService",
        "vpc-lattice:GetServiceNetwork",
        "vpc-lattice:GetTargetGroup",
        "vpc-lattice:ListAccessLogSubscriptions",
```

```
        "vpc-lattice:ListServiceNetworks",
        "vpc-lattice:ListServices",
        "vpc-lattice:ListTagsForResource",
        "vpc-lattice:ListTargetGroups",
        "vpc-lattice:ListTargets",
        "waf-regional:GetLoggingConfiguration",
        "waf-regional:GetWebACL",
        "waf-regional:GetWebACLForResource",
        "waf-regional:ListLoggingConfigurations",
        "waf:GetLoggingConfiguration",
        "waf:GetWebACL",
        "wafv2:GetLoggingConfiguration",
        "wafv2:GetRuleGroup",
        "wafv2:ListLoggingConfigurations",
        "wafv2:ListRuleGroups",
        "wafv2:ListTagsForResource",
        "workspaces:DescribeConnectionAliases",
        "workspaces:DescribeTags",
        "workspaces:DescribeWorkspaces",
        "xray:GetGroup",
        "xray:GetGroups",
        "xray:GetSamplingRules",
        "xray:ListResourcePolicies",
        "xray:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSConfigSLRLogStatementID",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/config/*"
    },
    {
      "Sid" : "AWSConfigSLRLogEventStatementID",
      "Effect" : "Allow",
      "Action" : "logs:PutLogEvents",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/config/*:log-stream:config-rule-
evaluation/*"
    },
    {
```

```
      "Sid" : "AWSConfigSLRApiGatewayStatementID",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/account",
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/apis/*/integrations",
        "arn:aws:apigateway:*::/apis/*/integrations/*",
        "arn:aws:apigateway:*::/domainnames",
        "arn:aws:apigateway:*::/domainnames/*",
        "arn:aws:apigateway:*::/clientcertificates",
        "arn:aws:apigateway:*::/clientcertificates/*",
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/resources",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integration",
        "arn:aws:apigateway:*::/restapis/*/resources/*",
        "arn:aws:apigateway:*::/usageplans",
        "arn:aws:apigateway:*::/usageplans/*",
        "arn:aws:apigateway:*::/apis/*/routes/*",
        "arn:aws:apigateway:*::/apis/*/routes",
        "arn:aws:apigateway:*::/v2/apis/*/routes",
        "arn:aws:apigateway:*::/v2/apis/*/routes/*",
        "arn:aws:apigateway:*::/v2/apis",
        "arn:aws:apigateway:*::/v2/apis/*",
        "arn:aws:apigateway:*::/v2/apis/*/integrations",
        "arn:aws:apigateway:*::/v2/apis/*/integrations/*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSConfigUserAccess

説明: リソースのタグによる検索やすべてのタグの読み取りなど、Config AWS を使用するためのアクセスを提供します。これは、管理者権限を必要とする Config AWS を設定するアクセス許可を提供しません。

AWSConfigUserAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSConfigUserAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 18 日 19:38 UTC
- 編集日時: 2019 年 3 月 18 日 20:27 UTC
- ARN: arn:aws:iam::aws:policy/AWSConfigUserAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSConnector

説明: AWS Connector がユーザーに代わって VMs をインポートできるように、すべての EC2 オブジェクトへの広範な読み取り/書き込みアクセス、「import-to-ec2-」で始まる S3 バケットへの読み取り/書き込みアクセス、およびすべての S3 バケットを一覧表示する機能を有効にします。

`AWSConnector` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSConnector` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 11 日 17:14 UTC
- 編集日時: 2015 年 9 月 28 日 19:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSConnector`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSControlTowerAccountServiceRolePolicy

説明: AWS Control Tower が自動アカウント設定と一元化されたガバナンスを提供する AWS サービスをユーザーに代わって呼び出すことを許可します。

`AWSControlTowerAccountServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 6 月 5 日 22:04 UTC
- 編集日時: 2025 年 11 月 5 日 23:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSControlTowerAccountServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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"
    },
    {
      "Sid" : "AllowDeleteConfigRule",
      "Effect" : "Allow",
      "Action" : [
        "config:DeleteConfigRule"
      ],
      "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/controltower.*/*"
    },
    {
      "Sid" : "AllowPutConfigRule",
      "Effect" : "Allow",
      "Action" : [
        "config:PutConfigRule"
      ],
```

```
      "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/controltower.*/*"
    },
    {
      "Sid" : "AllowConfigTagResource",
      "Effect" : "Allow",
      "Action" : [
        "config:TagResource"
      ],
      "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/controltower.*/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/aws-control-tower" : "managed-by-control-tower"
        }
      }
    },
    {
      "Sid" : "AllowConfigRulesDescribe",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigRules"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowControlTowerToCreateConfigAggregator",
      "Effect" : "Allow",
      "Action" : [
        "config:PutConfigurationAggregator"
      ],
      "Resource" : [
        "arn:aws:config:*:*:config-aggregator/aws-service-config-aggregator/
controltower.amazonaws.com/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowControlTowerToManageConfigAggregator",
      "Effect" : "Allow",
      "Action" : [
        "config:DeleteConfigurationAggregator",
```

```
        "config:DescribeAggregateComplianceByConfigRules",
        "config:SelectAggregateResourceConfig"
      ],
      "Resource" : [
        "arn:aws:config:*:*:config-aggregator/aws-service-config-aggregator/
controltower.amazonaws.com/config-aggregator-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowControlTowerToTagConfigAggregator",
      "Effect" : "Allow",
      "Action" : [
        "config:TagResource"
      ],
      "Resource" : [
        "arn:aws:config:*:*:config-aggregator/aws-service-config-aggregator/
controltower.amazonaws.com/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/aws-control-tower" : "managed-by-control-tower",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowControlTowerToPassAggregatorRoleToConfig",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/config.amazonaws.com/
AWSServiceRoleForConfig"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "config.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Sid" : "AllowDescribeConfigurationAggregators",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigurationAggregators"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowListDelegatedAdministratorsForConfig",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "config.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowListDescribeOrganization",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowActionsForCloudFormationHooksIntegration",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:SetTypeConfiguration",
        "cloudformation:DeactivateType",
```

```
        "cloudformation:ActivateType"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:type/hook/AWS-ControlTower*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSControlTowerCloudTrailRolePolicy

説明: AWS Control Tower はベストプラクティスとして AWS CloudTrail を有効にし、このロールを AWS CloudTrail に提供します。 AWS CloudTrail はCloudTrail ログを作成および公開するためにこのロールを引き受けます。

AWSControlTowerCloudTrailRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSControlTowerCloudTrailRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2025 年 11 月 5 日 21:19 UTC
- 編集日時: 2025 年 11 月 5 日 21:19 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSControlTowerCloudTrailRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "logs:CreateLogStream",
      "Resource" : "arn:aws:logs:*:*:log-group:aws-controltower/CloudTrailLogs*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:PutLogEvents",
      "Resource" : "arn:aws:logs:*:*:log-group:aws-controltower/CloudTrailLogs*:*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSControlTowerIdentityCenterManagementPolicy

説明: AWS Control Tower に登録されているメンバーアカウントの IAM Identity Center (IdC) リソースを管理するアクセス許可を提供します。ポリシーは、お客様が AWS Control Tower ランディングゾーンで IAM IdC 統合をオプトインした場合にのみ、AWSControlTowerAdmin ロールにアタッチされます。

`AWSControlTowerIdentityCenterManagementPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSControlTowerIdentityCenterManagementPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2025 年 10 月 3 日 18:34 UTC
- 編集日時: 2025 年 10 月 3 日 18:34 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSControlTowerIdentityCenterManagementPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowIdentityCenterInstancePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sso:ListPermissionSets"
      ],
      "Resource" : "arn:aws:sso:::instance/*"
    },
    {
      "Sid" : "AllowIdentityCenterManagementPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sso:DescribeRegisteredRegions",
        "sso:ListDirectoryAssociations",
```

```
        "sso:ListProfileAssociations",
        "sso:AssociateProfile",
        "sso:GetProfile",
        "sso:CreateProfile",
        "sso:UpdateProfile",
        "sso:GetTrust",
        "sso:CreateTrust",
        "sso:UpdateTrust",
        "sso:CreateApplicationInstance",
        "sso:GetApplicationInstance",
        "sso:GetSSOStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowIdentityCenterDirectoryPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:SearchGroups",
        "sso-directory:CreateGroup",
        "sso-directory:SearchUsers",
        "sso-directory:CreateUser",
        "sso-directory:DescribeDirectory"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSControlTowerServiceRolePolicy

説明: AWS Control Tower が管理または使用する AWS リソースへのアクセスを提供します

AWSControlTowerServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSControlTowerServiceRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2019 年 5 月 3 日 18:19 UTC
- 編集日時: 2025 年 11 月 5 日 22:49 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSControlTowerServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v13 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:CreateStackInstances",
        "cloudformation:CreateStackSet",
        "cloudformation:DeleteStack",
        "cloudformation:DeleteStackInstances",
        "cloudformation:DeleteStackSet",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:ListStackInstances",
```

```
        "cloudformation:UpdateStack",
        "cloudformation:UpdateStackInstances",
        "cloudformation:UpdateStackSet"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:type/resource/AWS-IAM-Role"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:CreateStackInstances",
        "cloudformation:CreateStackSet",
        "cloudformation:DeleteStack",
        "cloudformation:DeleteStackInstances",
        "cloudformation:DeleteStackSet",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:GetTemplate",
        "cloudformation:ListStackInstances",
        "cloudformation:UpdateStack",
        "cloudformation:UpdateStackInstances",
        "cloudformation:UpdateStackSet"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/AWSControlTower*/*",
        "arn:aws:cloudformation:*:*:stack/StackSet-AWSControlTower*/*",
        "arn:aws:cloudformation:*:*:stackset/AWSControlTower*:*",
        "arn:aws:cloudformation:*:*:stackset-target/AWSControlTower*/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateTrail",
        "cloudtrail:DeleteTrail",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:StartLogging",
        "cloudtrail:StopLogging",
        "cloudtrail:UpdateTrail",
        "cloudtrail:PutEventSelectors",
```

```
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:aws-controltower/CloudTrailLogs*:*",
        "arn:aws:cloudtrail:*:*:trail/aws-controltower*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-controltower*/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSControlTowerExecution",
        "arn:aws:iam::*:role/AWSControlTowerBlueprintAccess"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:DescribeTrails",
        "ec2:DescribeAvailabilityZones",
        "iam:ListRoles",
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups",
        "organizations:CreateAccount",
        "organizations:DescribeAccount",
        "organizations:DescribeCreateAccountStatus",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribePolicy",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
```

```
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListChildren",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListPoliciesForTarget",
        "organizations:ListTargetsForPolicy",
        "organizations:ListRoots",
        "organizations:MoveAccount",
        "servicecatalog:AssociatePrincipalWithPortfolio"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetUser",
        "iam:ListAttachedRolePolicies",
        "iam:GetRolePolicy"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AWSControlTowerStackSetRole",
        "arn:aws:iam::*:role/service-role/AWSControlTowerCloudTrailRole",
        "arn:aws:iam::*:role/service-role/
AWSControlTowerConfigAggregatorRoleForOrganizations"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DeleteConfigurationAggregator",
        "config:PutConfigurationAggregator",
        "config:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceTag/aws-control-tower" : "managed-by-control-tower"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:DisableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "organizations:ServicePrincipal" : [
            "config.amazonaws.com",
            "cloudtrail.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "cloudtrail.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "account:EnableRegion",
        "account:ListRegions",
        "account:GetRegionOptStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForCloudFormationHooksIntegration",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:SetTypeConfiguration",
```

```
        "cloudformation:DeactivateType",
        "cloudformation:ActivateType"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:type/hook/AWS-ControlTower*"
    },
    {
      "Sid" : "AllowActionsForCloudFormationStackSetOrganizationsTrustedAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ActivateOrganizationsAccess",
        "cloudformation:DescribeOrganizationsAccess"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSCostAndUsageReportAutomationPolicy

説明: アカウントの構成を説明し、MAP プログラム用の S3 バケットを作成してそれにタグを適用し、コストおよび使用状況レポートを作成し、コストおよび使用状況レポートの定義を説明する権限を付与します。

AWSCostAndUsageReportAutomationPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCostAndUsageReportAutomationPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー

- 作成日時: 2021 年 11 月 1 日 21:27 UTC
- 編集日時: 2021 年 11 月 1 日 21:27 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSCostAndUsageReportAutomationPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSDataExchangeDataGrantOwnerFullAccess

説明: AWS マネジメントコンソール および SDK を使用して Data Exchange アクションへのアクセス権を AWS Data Grant 所有者に付与します。

`AWSDataExchangeDataGrantOwnerFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSDataExchangeDataGrantOwnerFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 10 月 24 日 14:43 UTC
- 編集日時: 2024 年 10 月 24 日 14:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeDataGrantOwnerFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataExchangeActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:CreateDataSet",
        "dataexchange:UpdateDataSet",
        "dataexchange:GetDataSet",
        "dataexchange:DeleteDataSet",
        "dataexchange:ListDataSets",
        "dataexchange:CreateRevision",
        "dataexchange:UpdateRevision",
        "dataexchange:GetRevision",
        "dataexchange:DeleteRevision",
        "dataexchange:RevokeRevision",
        "dataexchange:ListDataSetRevisions",
        "dataexchange:CreateAsset",
        "dataexchange:UpdateAsset",
        "dataexchange:GetAsset",
        "dataexchange:DeleteAsset",
        "dataexchange:ListRevisionAssets",
        "dataexchange:SendApiAsset",
        "dataexchange:CreateDataGrant",
        "dataexchange:GetDataGrant",
        "dataexchange:DeleteDataGrant",
        "dataexchange:ListDataGrants",
        "dataexchange:PublishToDataGrant",
        "dataexchange:SendDataSetNotification",
        "dataexchange:TagResource",
        "dataexchange:UntagResource"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "DataExchangeJobsActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:CreateJob",
        "dataexchange:StartJob",
        "dataexchange:CancelJob"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "dataexchange:JobType" : [
            "IMPORT_ASSETS_FROM_S3",
            "IMPORT_ASSET_FROM_SIGNED_URL",
            "EXPORT_ASSETS_TO_S3",
            "EXPORT_ASSET_TO_SIGNED_URL",
            "IMPORT_ASSET_FROM_API_GATEWAY_API",
            "IMPORT_ASSETS_FROM_REDSHIFT_DATA_SHARES",
            "IMPORT_ASSETS_FROM_LAKE_FORMATION_TAG_POLICY"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSDataExchangeDataGrantReceiverFullAccess

説明: AWS マネジメントコンソール および SDK を使用して Data Exchange アクションへのアクセス権を AWS Data Grant レシーバーに付与します。

AWSDataExchangeDataGrantReceiverFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSDataExchangeDataGrantReceiverFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 10 月 24 日 14:45 UTC
- 編集日時: 2024 年 10 月 24 日 14:45 UTC
- ARN: arn:aws:iam::aws:policy/AWSDataExchangeDataGrantReceiverFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataExchangeReadOnlyActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:GetDataSet",
        "dataexchange:ListDataSets",
        "dataexchange:GetRevision",
        "dataexchange:ListDataSetRevisions",
        "dataexchange:GetAsset",
        "dataexchange:ListRevisionAssets",
        "dataexchange:SendApiAsset"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "DataExchangeExportActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:CreateJob",
        "dataexchange:StartJob",
        "dataexchange:CancelJob"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "dataexchange:JobType" : [
            "EXPORT_ASSETS_TO_S3",
            "EXPORT_ASSET_TO_SIGNED_URL",
            "EXPORT_REVISIONS_TO_S3"
          ]
        }
      }
    },
    {
      "Sid" : "DataExchangeEventActionActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:CreateEventAction",
        "dataexchange:UpdateEventAction",
        "dataexchange:DeleteEventAction",
        "dataexchange:GetEventAction",
        "dataexchange:ListEventActions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataExchangeDataGrantActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:AcceptDataGrant",
        "dataexchange:ListReceivedDataGrants",
        "dataexchange:GetReceivedDataGrant"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSDataExchangeFullAccess

説明: および SDK を使用して AWS Data Exchange AWS マネジメントコンソール および AWS Marketplace アクションへのフルアクセスを許可します。また、 AWS Data Exchange を最大限に活用するために必要な関連サービスへの選択アクセスも提供します。

`AWSDataExchangeFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSDataExchangeFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 11 月 13 日 19:27 UTC
- 編集日時: 2024 年 6 月 24 日 19:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataExchangeActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3GetActionConditionalResourceAndADX",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::*aws-data-exchange*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "S3GetActionConditionalTagAndADX",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/AWSDataExchange" : "true"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "S3WriteActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource" : "arn:aws:s3:::*aws-data-exchange*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "S3ReadActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSMarketplaceProviderActions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity",
        "aws-marketplace:ListEntities",
        "aws-marketplace:StartChangeSet",
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:CancelChangeSet",
        "aws-marketplace:GetAgreementApprovalRequest",
        "aws-marketplace:ListAgreementApprovalRequests",
        "aws-marketplace:AcceptAgreementApprovalRequest",
        "aws-marketplace:RejectAgreementApprovalRequest",
        "aws-marketplace:UpdateAgreementApprovalRequest",
        "aws-marketplace:SearchAgreements",
        "aws-marketplace:GetAgreementTerms",
        "aws-marketplace:TagResource",
        "aws-marketplace:UntagResource",
```

```
        "aws-marketplace:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSMarketplaceSubscriberActions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:Subscribe",
        "aws-marketplace:Unsubscribe",
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:GetAgreementRequest",
        "aws-marketplace:ListAgreementRequests",
        "aws-marketplace:CancelAgreementRequest",
        "aws-marketplace:ListPrivateListings",
        "aws-marketplace:DescribeAgreement"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSActions",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListKeys"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftConditionalActions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:AuthorizeDataShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "redshift:ConsumerIdentifier" : "ADX"
        }
      }
    },
    {
      "Sid" : "RedshiftActions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeDataSharesForProducer",
        "redshift:DescribeDataShares"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "APIGatewayActions",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSDataExchangeProviderFullAccess

説明: AWS マネジメントコンソール および SDK を使用して AWS Data Exchange および AWS Marketplace アクションへのアクセス権をデータプロバイダーに付与します。また、 AWS Data Exchange を最大限に活用するために必要な関連サービスへの選択アクセスも提供します。

`AWSDataExchangeProviderFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSDataExchangeProviderFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 11 月 13 日 19:27 UTC
- 編集日時: 2024 年 8 月 15 日 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeProviderFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v12 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataExchangeActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:CreateDataSet",
        "dataexchange:CreateRevision",
        "dataexchange:CreateAsset",
        "dataexchange:Get*",
        "dataexchange:Update*",
        "dataexchange:List*",
        "dataexchange:Delete*",
        "dataexchange:TagResource",
        "dataexchange:UntagResource",
        "dataexchange:PublishDataSet",
        "dataexchange:SendApiAsset",
        "dataexchange:RevokeRevision",
        "dataexchange:SendDataSetNotification",
        "tag:GetTagKeys",
        "tag:GetTagValues"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "DataExchangeJobsActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:CreateJob",
        "dataexchange:StartJob",
        "dataexchange:CancelJob"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "dataexchange:JobType" : [
            "IMPORT_ASSETS_FROM_S3",
            "IMPORT_ASSET_FROM_SIGNED_URL",
            "EXPORT_ASSETS_TO_S3",
            "EXPORT_ASSET_TO_SIGNED_URL",
            "IMPORT_ASSET_FROM_API_GATEWAY_API",
            "IMPORT_ASSETS_FROM_REDSHIFT_DATA_SHARES"
          ]
        }
      }
    },
    {
      "Sid" : "S3GetActionConditionalResourceAndADX",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::*aws-data-exchange*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "S3GetActionConditionalTagAndADX",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
```

```
          "s3:ExistingObjectTag/AWSDataExchange" : "true"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "S3WriteActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource" : "arn:aws:s3:::*aws-data-exchange*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "S3ReadActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSMarketplaceActions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity",
        "aws-marketplace:ListEntities",
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:StartChangeSet",
```

```
        "aws-marketplace:CancelChangeSet",
        "aws-marketplace:GetAgreementApprovalRequest",
        "aws-marketplace:ListAgreementApprovalRequests",
        "aws-marketplace:AcceptAgreementApprovalRequest",
        "aws-marketplace:RejectAgreementApprovalRequest",
        "aws-marketplace:UpdateAgreementApprovalRequest",
        "aws-marketplace:SearchAgreements",
        "aws-marketplace:GetAgreementTerms"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSActions",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListKeys"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftConditionalActions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:AuthorizeDataShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "redshift:ConsumerIdentifier" : "ADX"
        }
      }
    },
    {
      "Sid" : "RedshiftActions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeDataSharesForProducer",
        "redshift:DescribeDataShares"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "APIGatewayActions",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSDataExchangeReadOnly

説明: AWS マネジメントコンソール および SDK を使用して AWS Data Exchange および AWS Marketplace アクションへの読み取り専用アクセスを許可します。

`AWSDataExchangeReadOnly` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSDataExchangeReadOnly` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 11 月 13 日 19:27 UTC
- 編集日時: 2024 年 10 月 24 日 14:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeReadOnly`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataExchangeReadOnlyActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:GetAsset",
        "dataexchange:GetDataSet",
        "dataexchange:GetEventAction",
        "dataexchange:GetJob",
        "dataexchange:GetRevision",
        "dataexchange:GetDataGrant",
        "dataexchange:GetReceivedDataGrant",
        "dataexchange:ListDataGrants",
        "dataexchange:ListReceivedDataGrants",
        "dataexchange:ListDataSetRevisions",
        "dataexchange:ListDataSets",
        "dataexchange:ListEventActions",
        "dataexchange:ListJobs",
        "dataexchange:ListRevisionAssets",
        "dataexchange:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSMarketplaceReadOnlyActions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:GetAgreementRequest",
        "aws-marketplace:ListAgreementRequests",
        "aws-marketplace:GetAgreementApprovalRequest",
        "aws-marketplace:ListAgreementApprovalRequests",
        "aws-marketplace:DescribeEntity",
        "aws-marketplace:ListEntities",
        "aws-marketplace:DescribeChangeSet",
```

```
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:SearchAgreements",
        "aws-marketplace:GetAgreementTerms",
        "aws-marketplace:ListPrivateListings",
        "aws-marketplace:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSDataExchangeServiceRolePolicyForLicenseManagement

説明: AWS Data Exchange がライセンス管理のために AWS Data Exchange が使用または管理する AWS のサービス および リソースにアクセスできるようにします。

`AWSDataExchangeServiceRolePolicyForLicenseManagement` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2024 年 10 月 10 日 14:54 UTC
- 編集日時: 2024 年 10 月 10 日 14:54 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowLicenseManagerActions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "license-manager:ListDistributedGrants",
        "license-manager:GetGrant",
        "license-manager:CreateGrantVersion",
        "license-manager:DeleteGrant"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSDataExchangeServiceRolePolicyForOrganizationDiscovery

説明: AWS Data Exchange が AWS Organization に関するデータを読み取って AWS 、Data Exchange データ付与ライセンス配布の適格性を判断できるようにします。

AWSDataExchangeServiceRolePolicyForOrganizationDiscovery は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2024 年 10 月 10 日 14:33 UTC
- 編集日時: 2024 年 10 月 10 日 14:33 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSDataExchangeServiceRolePolicyForOrganizationDiscovery

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "organizations:ListAccounts"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSDataExchangeSubscriberFullAccess

説明: AWS マネジメントコンソール および SDK を使用して AWS Data Exchange および AWS Marketplace アクションへのアクセスをデータサブスクライバーに付与します。また、 AWS Data Exchange を最大限に活用するために必要な関連サービスへの選択アクセスも提供します。

`AWSDataExchangeSubscriberFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSDataExchangeSubscriberFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 11 月 13 日 19:27 UTC
- 編集日時: 2024 年 5 月 21 日 17:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeSubscriberFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント


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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSDataLifecycleManagerServiceRole

説明: AWS リソースに対してアクションを実行するための適切なアクセス許可を AWS Data Lifecycle Manager に提供します

`AWSDataLifecycleManagerServiceRole` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSDataLifecycleManagerServiceRole` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2018 年 7 月 6 日 19:34 UTC

- 編集日時: 2024 年 12 月 16 日 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDataLifecycleManagerServiceRole`

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot",
        "ec2:CreateSnapshots",
        "ec2:DeleteSnapshot",
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots",
        "ec2:EnableFastSnapshotRestores",
        "ec2:DescribeFastSnapshotRestores",
        "ec2:DisableFastSnapshotRestores",
        "ec2:CopySnapshot",
        "ec2:ModifySnapshotAttribute",
        "ec2:DescribeSnapshotAttribute",
        "ec2:DescribeSnapshotTierStatus",
        "ec2:ModifySnapshotTier",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:DeleteRule",
        "events:DescribeRule",
        "events:EnableRule",
        "events:DisableRule",
        "events:ListTargetsByRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/AwsDataLifecycleRule.managed-cwe.*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSDataLifecycleManagerServiceRoleForAMIManagement

説明: AMI Management の AWS リソースに対してアクションを実行するための適切なアクセス許可を AWS Data Lifecycle Manager に提供します。

`AWSDataLifecycleManagerServiceRoleForAMIManagement` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSDataLifecycleManagerServiceRoleForAMIManagement` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 10 月 21 日 19:39 UTC
- 編集日時: 2021 年 8 月 19 日 17:03 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDataLifecycleManagerServiceRoleForAMIManagement`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSDataLifecycleManagerSSMFullAccess

説明: すべての Amazon EC2 インスタンスで事前スクリプトと事後スクリプトを実行するために必要な Systems Manager アクションを実行する権限を Amazon Data Lifecycle Manager に付与します。

`AWSDataLifecycleManagerSSMFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSDataLifecycleManagerSSMFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 10 月 31 日 20:29 UTC
- 編集日時: 2023 年 11 月 16 日 22:31 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSDataLifecycleManagerSSMFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSDataPipeline_FullAccess

説明: Data Pipeline へのフルアクセス、S3、DynamoDB、Redshift、RDS、SNS、IAM ロールへのリストアクセス、およびデフォルトロールの passRole アクセスを提供します。

`AWSDataPipeline_FullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSDataPipeline_FullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 1 月 19 日 23:14 UTC
- 編集日時: 2017 年 8 月 17 日 18:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataPipeline_FullAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSDataPipeline_PowerUser

説明: Data Pipeline へのフルアクセス、S3、DynamoDB、Redshift、RDS、SNS、IAM ロールへのリストアクセス、およびデフォルトロールの passRole アクセスを提供します。

AWSDataPipeline_PowerUser は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSDataPipeline_PowerUser をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 1 月 19 日 23:16 UTC
- 編集日時: 2017 年 8 月 17 日 18:49 UTC
- ARN: arn:aws:iam::aws:policy/AWSDataPipeline_PowerUser

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSDataSyncDiscoveryServiceRolePolicy

説明: DataSync Discovery がユーザーに代わって他の AWS サービスと統合できるようにします。

`AWSDataSyncDiscoveryServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー

- 作成日時: 2023 年 3 月 20 日 22:19 UTC
- 編集日時: 2023 年 3 月 20 日 22:19 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSDataSyncDiscoveryServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSDataSyncFullAccess

説明: AWS DataSync へのフルアクセスと依存関係への最小限のアクセスを提供します

`AWSDataSyncFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSDataSyncFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 1 月 18 日 19:40 UTC
- 編集日時: 2025 年 5 月 20 日 19:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataSyncFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v10 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataSyncFullAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "datasync:*",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRegions",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpoints",
        "ec2:ModifyNetworkInterfaceAttribute",
        "fsx:DescribeFileSystems",
        "fsx:DescribeStorageVirtualMachines",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets",
        "iam:GetRole",
        "iam:ListRoles",
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups",
        "logs:DescribeResourcePolicies",
        "outposts:ListOutposts",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3-outposts:ListAccessPoints",
        "s3-outposts:ListRegionalBuckets",
        "secretsmanager:ListSecrets",
        "kms:ListAliases",
        "kms:DescribeKey"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataSyncPassRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "datasync.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DataSyncCreateSLRPermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/datasync.amazonaws.com/
AWSServiceRoleForDataSync",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "datasync.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DataSyncSecretsManagerCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : [
        "arn:*:secretsmanager:*:*:secret:aws-datasync!*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Sid" : "DataSyncSecretsManagerAccess",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DeleteSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : [
        "arn:*:secretsmanager:*:*:secret:aws-datasync!*"
      ],
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "aws-
datasync",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSDataSyncReadOnlyAccess

説明: AWS DataSync への読み取り専用アクセスを提供します

`AWSDataSyncReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSDataSyncReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 1 月 18 日 19:18 UTC
- 編集日時: 2020 年 6 月 30 日 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataSyncReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSDataSyncServiceRolePolicy

説明: DataSync がユーザーに代わって他の AWS サービスと統合することを許可する

`AWSDataSyncServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2024 年 10 月 9 日 17:45 UTC
- 編集日時: 2025 年 4 月 15 日 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDataSyncServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataSyncCloudWatchLogCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream"
      ],
      "Resource" : [
        "arn:*:logs:*:*:log-group:/aws/datasync*"
      ]
    },
    {
      "Sid" : "DataSyncCloudWatchLogStreamUpdateAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:*:logs:*:*:log-group:/aws/datasync*:log-stream:*"
      ]
    },
    {
      "Sid" : "DataSyncSecretsManagerReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : [
        "arn:*:secretsmanager:*:*:secret:aws-datasync!*"
      ],
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "aws-
datasync",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSDeadlineCloud-FleetWorker

説明: Deadline Cloud AWS ワーカーにファームでタスクを実行するためのアクセスを提供します。

AWSDeadlineCloud-FleetWorker は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSDeadlineCloud-FleetWorker をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 4 月 1 日 17:21 UTC
- 編集日時: 2024 年 4 月 1 日 17:21 UTC
- ARN: arn:aws:iam::aws:policy/AWSDeadlineCloud-FleetWorker

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSDeadlineCloud-UserAccessFarms

説明: Deadline Cloud AWS ファームへのユーザーワークステーションアクセスに、他の必要なサービスを呼び出すための制限された読み取り専用アクセス許可を付与します。このポリシーをスタジオに関連付けられているユーザーロールにアタッチしてください。

AWSDeadlineCloud-UserAccessFarms は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSDeadlineCloud-UserAccessFarms をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 4 月 1 日 16:54 UTC
- 編集日時: 2024 年 10 月 7 日 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeadlineCloud-UserAccessFarms`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AdditionalPermissions",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeGroup",
        "identitystore:DescribeUser",
        "identitystore:ListGroupMembershipsForMember",
        "deadline:GetApplicationVersion",
        "ec2:DescribeInstanceTypes",
        "identitystore:ListUsers"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "OwnerLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssociateMemberToFarm",
```

```
        "deadline:AssociateMemberToFleet",
        "deadline:AssociateMemberToJob",
        "deadline:AssociateMemberToQueue",
        "deadline:CreateBudget",
        "deadline:DeleteBudget",
        "deadline:DisassociateMemberFromFarm",
        "deadline:DisassociateMemberFromFleet",
        "deadline:DisassociateMemberFromJob",
        "deadline:DisassociateMemberFromQueue",
        "deadline:GetBudget",
        "deadline:GetSessionsStatisticsAggregation",
        "deadline:ListBudgets",
        "deadline:StartSessionsStatisticsAggregation",
        "deadline:UpdateBudget"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:FarmMembershipLevels" : [
            "OWNER"
          ]
        }
      }
    },
    {
      "Sid" : "ManagerLevelMemberAssociation",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssociateMemberToFarm",
        "deadline:AssociateMemberToFleet",
        "deadline:AssociateMemberToJob",
        "deadline:AssociateMemberToQueue"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:FarmMembershipLevels" : [
            "MANAGER"
          ]
        },
```

```
        "StringEquals" : {
          "deadline:AssociatedMembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER",
            ""
          ],
          "deadline:MembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER"
          ]
        }
      }
    },
    {
      "Sid" : "ManagerLevelMemberDisassociation",
      "Effect" : "Allow",
      "Action" : [
        "deadline:DisassociateMemberFromFarm",
        "deadline:DisassociateMemberFromFleet",
        "deadline:DisassociateMemberFromJob",
        "deadline:DisassociateMemberFromQueue"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:FarmMembershipLevels" : [
            "MANAGER"
          ]
        },
        "StringEquals" : {
          "deadline:AssociatedMembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER",
            ""
          ]
        }
      }
    },
    {
```

```
      "Sid" : "OwnerManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:ListFarmMembers",
        "deadline:ListFleetMembers",
        "deadline:ListJobMembers",
        "deadline:ListQueueMembers",
        "deadline:UpdateJob",
        "deadline:UpdateSession",
        "deadline:UpdateStep",
        "deadline:UpdateTask"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:FarmMembershipLevels" : [
            "OWNER",
            "MANAGER"
          ]
        }
      }
    },
    {
      "Sid" : "OwnerManagerContributorPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssumeQueueRoleForUser",
        "deadline:CreateJob"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:FarmMembershipLevels" : [
            "OWNER",
            "MANAGER",
            "CONTRIBUTOR"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "AllLevelsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssumeFleetRoleForRead",
        "deadline:AssumeQueueRoleForRead",
        "deadline:GetFarm",
        "deadline:GetFleet",
        "deadline:GetJob",
        "deadline:GetJobTemplate",
        "deadline:GetQueue",
        "deadline:GetQueueEnvironment",
        "deadline:GetQueueFleetAssociation",
        "deadline:GetSession",
        "deadline:GetSessionAction",
        "deadline:GetStep",
        "deadline:GetStorageProfile",
        "deadline:GetStorageProfileForQueue",
        "deadline:GetTask",
        "deadline:GetWorker",
        "deadline:ListJobParameterDefinitions",
        "deadline:ListQueueEnvironments",
        "deadline:ListQueueFleetAssociations",
        "deadline:ListSessionActions",
        "deadline:ListSessions",
        "deadline:ListSessionsForWorker",
        "deadline:ListStepConsumers",
        "deadline:ListStepDependencies",
        "deadline:ListSteps",
        "deadline:ListStorageProfiles",
        "deadline:ListStorageProfilesForQueue",
        "deadline:ListTasks",
        "deadline:ListWorkers",
        "deadline:SearchJobs",
        "deadline:SearchSteps",
        "deadline:SearchTasks",
        "deadline:SearchWorkers"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:FarmMembershipLevels" : [
```

```
            "OWNER",
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER"
          ]
        }
      }
    },
    {
      "Sid" : "ListBasedOnMembership",
      "Effect" : "Allow",
      "Action" : [
        "deadline:ListFarms",
        "deadline:ListFleets",
        "deadline:ListJobs",
        "deadline:ListQueues"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "deadline:RequesterPrincipalId" : "${deadline:PrincipalId}"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSDeadlineCloud-UserAccessFleets

説明: Deadline Cloud AWS フリートへのユーザーワークステーションアクセスに、他の必要なサービスを呼び出すための制限された読み取り専用アクセス許可を付与します。このポリシーをスタジオに関連付けられているユーザーロールにアタッチしてください。

AWSDeadlineCloud-UserAccessFleets は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSDeadlineCloud-UserAccessFleets をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 4 月 1 日 17:01 UTC
- 編集日時: 2024 年 4 月 1 日 17:01 UTC
- ARN: arn:aws:iam::aws:policy/AWSDeadlineCloud-UserAccessFleets

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSDeadlineCloud-UserAccessJobs

説明: Deadline Cloud AWS ジョブへのユーザーワークステーションアクセスに、他の必要なサービスを呼び出すための制限された読み取り専用アクセス許可を付与します。このポリシーをスタジオに関連付けられているユーザーロールにアタッチしてください。

AWSDeadlineCloud-UserAccessJobs は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSDeadlineCloud-UserAccessJobs をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 4 月 1 日 17:05 UTC
- 編集日時: 2024 年 10 月 7 日 18:24 UTC
- ARN: arn:aws:iam::aws:policy/AWSDeadlineCloud-UserAccessJobs

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AdditionalPermissions",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeGroup",
        "identitystore:DescribeUser",
        "identitystore:ListGroupMembershipsForMember",
        "deadline:GetApplicationVersion",
        "ec2:DescribeInstanceTypes",
        "identitystore:ListUsers"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "OwnerLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssociateMemberToJob",
        "deadline:DisassociateMemberFromJob"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:JobMembershipLevels" : [
            "OWNER"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "ManagerLevelMemberAssociation",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssociateMemberToJob"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:JobMembershipLevels" : [
            "MANAGER"
          ]
        },
        "StringEquals" : {
          "deadline:AssociatedMembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER",
            ""
          ],
          "deadline:MembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER"
          ]
        }
      }
    },
    {
      "Sid" : "ManagerLevelMemberDisassociation",
      "Effect" : "Allow",
      "Action" : [
        "deadline:DisassociateMemberFromJob"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
```

```
          "deadline:JobMembershipLevels" : [
            "MANAGER"
          ]
        },
        "StringEquals" : {
          "deadline:AssociatedMembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER",
            ""
          ]
        }
      }
    },
    {
      "Sid" : "OwnerManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:ListJobMembers",
        "deadline:UpdateJob",
        "deadline:UpdateSession",
        "deadline:UpdateStep",
        "deadline:UpdateTask"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:JobMembershipLevels" : [
            "OWNER",
            "MANAGER"
          ]
        }
      }
    },
    {
      "Sid" : "AllLevelsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:GetJob",
        "deadline:GetJobTemplate",
        "deadline:GetSession",
        "deadline:GetSessionAction",
```

```
        "deadline:GetStep",
        "deadline:GetTask",
        "deadline:ListJobParameterDefinitions",
        "deadline:ListSessionActions",
        "deadline:ListSessions",
        "deadline:ListStepConsumers",
        "deadline:ListStepDependencies",
        "deadline:ListSteps",
        "deadline:ListTasks",
        "deadline:SearchSteps",
        "deadline:SearchTasks"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:JobMembershipLevels" : [
            "OWNER",
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER"
          ]
        }
      }
    },
    {
      "Sid" : "ListBasedOnMembership",
      "Effect" : "Allow",
      "Action" : [
        "deadline:ListJobs"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "deadline:RequesterPrincipalId" : "${deadline:PrincipalId}"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSDeadlineCloud-UserAccessQueues

説明: Deadline Cloud AWS キューへのユーザーワークステーションアクセスに、他の必要なサービスを呼び出すための制限された読み取り専用アクセス許可を付与します。このポリシーをスタジオに関連付けられているユーザーロールにアタッチしてください。

`AWSDeadlineCloud-UserAccessQueues` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSDeadlineCloud-UserAccessQueues` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 4 月 1 日 17:10 UTC
- 編集日時: 2024 年 10 月 7 日 18:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeadlineCloud-UserAccessQueues`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AdditionalPermissions",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeGroup",
        "identitystore:DescribeUser",
        "identitystore:ListGroupMembershipsForMember",
        "deadline:GetApplicationVersion",
        "ec2:DescribeInstanceTypes",
        "identitystore:ListUsers"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "OwnerLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssociateMemberToJob",
        "deadline:AssociateMemberToQueue",
        "deadline:DisassociateMemberFromJob",
        "deadline:DisassociateMemberFromQueue"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:QueueMembershipLevels" : [
            "OWNER"
          ]
        }
      }
    },
    {
      "Sid" : "ManagerLevelMemberAssociation",
      "Effect" : "Allow",
```

```
      "Action" : [
        "deadline:AssociateMemberToJob",
        "deadline:AssociateMemberToQueue"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:QueueMembershipLevels" : [
            "MANAGER"
          ]
        },
        "StringEquals" : {
          "deadline:AssociatedMembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER",
            ""
          ],
          "deadline:MembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER"
          ]
        }
      }
    },
    {
      "Sid" : "ManagerLevelMemberDisassociation",
      "Effect" : "Allow",
      "Action" : [
        "deadline:DisassociateMemberFromJob",
        "deadline:DisassociateMemberFromQueue"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:QueueMembershipLevels" : [
            "MANAGER"
          ]
        },
```

```
        "StringEquals" : {
          "deadline:AssociatedMembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER",
            ""
          ]
        }
      }
    },
    {
      "Sid" : "OwnerManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:ListJobMembers",
        "deadline:ListQueueMembers",
        "deadline:UpdateJob",
        "deadline:UpdateSession",
        "deadline:UpdateStep",
        "deadline:UpdateTask"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:QueueMembershipLevels" : [
            "OWNER",
            "MANAGER"
          ]
        }
      }
    },
    {
      "Sid" : "OwnerManagerContributorPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssumeQueueRoleForUser",
        "deadline:CreateJob"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
```

```
        "ForAnyValue:StringEquals" : {
          "deadline:QueueMembershipLevels" : [
            "OWNER",
            "MANAGER",
            "CONTRIBUTOR"
          ]
        }
      }
    },
    {
      "Sid" : "AllLevelsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssumeQueueRoleForRead",
        "deadline:GetJob",
        "deadline:GetJobTemplate",
        "deadline:GetQueue",
        "deadline:GetQueueEnvironment",
        "deadline:GetQueueFleetAssociation",
        "deadline:GetSession",
        "deadline:GetSessionAction",
        "deadline:GetStep",
        "deadline:GetStorageProfileForQueue",
        "deadline:GetTask",
        "deadline:ListJobParameterDefinitions",
        "deadline:ListQueueEnvironments",
        "deadline:ListQueueFleetAssociations",
        "deadline:ListSessionActions",
        "deadline:ListSessions",
        "deadline:ListStepConsumers",
        "deadline:ListStepDependencies",
        "deadline:ListSteps",
        "deadline:ListStorageProfilesForQueue",
        "deadline:ListTasks",
        "deadline:SearchJobs",
        "deadline:SearchSteps",
        "deadline:SearchTasks"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:QueueMembershipLevels" : [
```

```
            "OWNER",
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER"
          ]
        }
      }
    },
    {
      "Sid" : "ListBasedOnMembership",
      "Effect" : "Allow",
      "Action" : [
        "deadline:ListJobs",
        "deadline:ListQueues"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "deadline:RequesterPrincipalId" : "${deadline:PrincipalId}"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSDeadlineCloud-WorkerHost

説明: AWS Deadline Cloud ワーカーホストがファーム内のフリートに参加するためのアクセスを提供します。

`AWSDeadlineCloud-WorkerHost` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSDeadlineCloud-WorkerHost をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 4 月 1 日 17:28 UTC
- 編集日時: 2025 年 4 月 30 日 17:07 UTC
- ARN: arn:aws:iam::aws:policy/AWSDeadlineCloud-WorkerHost

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "JoinFleetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:CreateWorker",
        "deadline:AssumeFleetRoleForWorker"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    },
    {
      "Sid" : "TagWorkerPermission",
```

```
      "Effect" : "Allow",
      "Action" : [
        "deadline:TagResource"
      ],
      "Resource" : "arn:aws:deadline:*:*:farm/*/fleet/*/worker/*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}",
          "deadline:CalledAction" : "CreateWorker"
        }
      }
    },
    {
      "Sid" : "ListFleetTagsPermission",
      "Effect" : "Allow",
      "Action" : [
        "deadline:ListTagsForResource"
      ],
      "Resource" : "arn:aws:deadline:*:*:farm/*/fleet/*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}",
          "deadline:CalledAction" : "CreateWorker"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSDeepLensLambdaFunctionAccessPolicy

説明:このポリシーは、DeepLens デバイス上で実行される DeepLens 管理用 Lambda 関数に必要な権限を指定します

AWSDeepLensLambdaFunctionAccessPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSDeepLensLambdaFunctionAccessPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 11 月 29 日 15:47 UTC
- 編集日時: 2019 年 6 月 11 日 23:11 UTC
- ARN: arn:aws:iam::aws:policy/AWSDeepLensLambdaFunctionAccessPolicy

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSDeepLensServiceRolePolicy

説明: AWS DeepLens に必要なリソースとロール、および IoT AWS のサービス、S3、GreenGrass、 AWS Lambda などの依存関係へのアクセス権を DeepLens に付与します。

AWSDeepLensServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSDeepLensServiceRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2017 年 11 月 29 日 15:46 UTC
- 編集日時: 2019 年 9 月 25 日 19:25 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSDeepLensServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSDeepRacerAccountAdminAccess

説明: DeepRacer の管理者は、マルチユーザーモードとシングルユーザーモードの切り替えを含むすべてのアクションにアクセスできます。

AWSDeepRacerAccountAdminAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSDeepRacerAccountAdminAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 10 月 28 日 01:27 UTC
- 編集日時: 2021 年 10 月 28 日 01:27 UTC
- ARN: arn:aws:iam::aws:policy/AWSDeepRacerAccountAdminAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
      "Condition" : {
        "Null" : {
          "deepracer:UserToken" : "true"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSDeepRacerCloudFormationAccessPolicy

説明: CloudFormation がユーザーに代わって AWS スタックとリソースを作成および管理できるようにします。

AWSDeepRacerCloudFormationAccessPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSDeepRacerCloudFormationAccessPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 2 月 28 日 21:59 UTC
- 編集日時: 2019 年 6 月 14 日 17:02 UTC
- ARN: arn:aws:iam::aws:policy/AWSDeepRacerCloudFormationAccessPolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSDeepRacerDefaultMultiUserAccess

説明: マルチユーザーで Deepracer を使用するための DeepRacer MultiUser デフォルトユーザーアクセス権

`AWSDeepRacerDefaultMultiUserAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSDeepRacerDefaultMultiUserAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 10 月 28 日 01:27 UTC
- 編集日時: 2021 年 10 月 28 日 01:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerDefaultMultiUserAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
```

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSDeepRacerFullAccess

説明: AWS DeepRacer へのフルアクセスを提供します。また、関連サービス (S3 など) への限定アクセスも提供します。

`AWSDeepRacerFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSDeepRacerFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 10 月 5 日 22:03 UTC
- 編集日時: 2020 年 10 月 5 日 22:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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-*/*"
```

```
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSDeepRacerRoboMakerAccessPolicy

説明: RoboMaker がユーザーに代わって必要なリソースを作成し、 AWS サービスを呼び出すことを許可します。

`AWSDeepRacerRoboMakerAccessPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSDeepRacerRoboMakerAccessPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 2 月 28 日 21:59 UTC
- 編集日時: 2019 年 2 月 28 日 21:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerRoboMakerAccessPolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSDeepRacerServiceRolePolicy

説明: DeepRacer がユーザーに代わって必要なリソースを作成し、 AWS サービスを呼び出すことを許可します。

AWSDeepRacerServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSDeepRacerServiceRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2019 年 2 月 28 日 21:58 UTC
- 編集日時: 2019 年 6 月 12 日 20:55 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSDeepRacerServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSDenyAll

説明: すべてのアクセスを拒否します。

AWSDenyAll は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSDenyAll をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 5 月 1 日 22:36 UTC
- 編集日時: 2023 年 12 月 18 日 16:42 UTC
- ARN: arn:aws:iam::aws:policy/AWSDenyAll

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
    {
      "Sid" : "DenyAll",
      "Effect" : "Deny",
      "Action" : [
        "*"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSDeviceFarmFullAccess

説明: すべての AWS Device Farm オペレーションへのフルアクセスを提供します。

`AWSDeviceFarmFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSDeviceFarmFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 7 月 13 日 16:37 UTC
- 編集日時: 2015 年 7 月 13 日 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeviceFarmFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSDeviceFarmServiceRolePolicy

説明: ユーザーに代わって EC2 Network APIs を呼び出すアクセス許可を AWS Device Farm に付与します。

`AWSDeviceFarmServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 9 月 20 日 21:02 UTC
- 編集日時: 2022 年 9 月 20 日 21:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDeviceFarmServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSDeviceFarmTestGridServiceRolePolicy

説明: ユーザーに代わって EC2 APIs を呼び出すアクセス許可を AWS Device Farm に付与します。

`AWSDeviceFarmTestGridServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー

- 作成日時: 2021 年 5 月 26 日 22:01 UTC
- 編集日時: 2021 年 5 月 26 日 22:01 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSDeviceFarmTestGridServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSDirectConnectFullAccess

説明: 経由で AWS Direct Connect へのフルアクセスを提供します AWS マネジメントコンソール。

`AWSDirectConnectFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSDirectConnectFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2019 年 4 月 30 日 15:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectConnectFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "directconnect:*",
        "ec2:DescribeVpnGateways",
        "ec2:DescribeTransitGateways"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSDirectConnectReadOnlyAccess

説明: 経由で AWS Direct Connect への読み取り専用アクセスを提供します AWS マネジメントコンソール。

`AWSDirectConnectReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSDirectConnectReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2020 年 5 月 18 日 18:48 UTC
- ARN: arn:aws:iam::aws:policy/AWSDirectConnectReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "directconnect:Describe*",
        "directconnect:List*",
        "ec2:DescribeVpnGateways",
        "ec2:DescribeTransitGateways"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSDirectConnectServiceRolePolicy

説明: ユーザーに代わって AWS リソースを作成および管理するための AWS Direct Connect アクセス許可を提供します。

`AWSDirectConnectServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 1 月 14 日 18:35 UTC
- 編集日時: 2021 年 1 月 14 日 18:35 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDirectConnectServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:ListSecretVersionIds",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:*directconnect*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSDirectoryServiceDataFullAccess

説明: AWS Directory Service Data へのフルアクセスを提供します。

`AWSDirectoryServiceDataFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSDirectoryServiceDataFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 9 月 18 日 21:45 UTC

- 編集日時: 2024 年 9 月 18 日 21:45 UTC
- ARN: arn:aws:iam::aws:policy/AWSDirectoryServiceDataFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DSDataFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "ds:AccessDSData",
        "ds-data:AddGroupMember",
        "ds-data:CreateGroup",
        "ds-data:CreateUser",
        "ds-data:DeleteGroup",
        "ds-data:DeleteUser",
        "ds-data:DescribeGroup",
        "ds-data:DescribeUser",
        "ds-data:DisableUser",
        "ds-data:ListGroupMembers",
        "ds-data:ListGroups",
        "ds-data:ListGroupsForMember",
        "ds-data:ListUsers",
        "ds-data:RemoveGroupMember",
        "ds-data:SearchGroups",
        "ds-data:SearchUsers",
        "ds-data:UpdateGroup",
        "ds-data:UpdateUser"
      ],
      "Resource" : [
        "arn:aws:ds:*:*:directory/*"
```

```
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSDirectoryServiceDataReadOnlyAccess

説明: AWS Directory Service Data への読み取り専用アクセスを提供します

`AWSDirectoryServiceDataReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSDirectoryServiceDataReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 9 月 18 日 22:00 UTC
- 編集日時: 2024 年 9 月 18 日 22:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectoryServiceDataReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DSDataReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "ds:AccessDSData",
        "ds-data:DescribeGroup",
        "ds-data:DescribeUser",
        "ds-data:ListGroupMembers",
        "ds-data:ListGroups",
        "ds-data:ListGroupsForMember",
        "ds-data:ListUsers",
        "ds-data:SearchGroups",
        "ds-data:SearchUsers"
      ],
      "Resource" : [
        "arn:aws:ds:*:*:directory/*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSDirectoryServiceFullAccess

説明: AWS Directory Service へのフルアクセスを提供します。

`AWSDirectoryServiceFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSDirectoryServiceFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2024 年 4 月 2 日 20:38 UTC
- ARN: arn:aws:iam::aws:policy/AWSDirectoryServiceFullAccess

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSDirectoryServiceReadOnlyAccess

説明: AWS Directory Service への読み取り専用アクセスを提供します。

`AWSDirectoryServiceReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSDirectoryServiceReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2018 年 9 月 25 日 21:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectoryServiceReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSDirectoryServiceServiceRolePolicy

説明: Directory Service のサービスにリンクされたロールのポリシー

AWSDirectoryServiceServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2025 年 7 月 11 日 00:22 UTC
- 編集日時: 2025 年 7 月 11 日 00:22 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSDirectoryServiceServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
    {
      "Sid" : "SSMSendCommandPermission",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-RunPowerShellScript",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Sid" : "EC2DescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMManagementPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListCommands",
        "ssm:GetCommandInvocation",
        "ssm:DescribeInstanceInformation",
        "ssm:GetConnectionStatus"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSDiscoveryContinuousExportFirehosePolicy

説明: AWS Discovery Continuous Export に必要な AWS リソースへの書き込みアクセスを提供します

AWSDiscoveryContinuousExportFirehosePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSDiscoveryContinuousExportFirehosePolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 8 月 9 日 18:29 UTC
- 編集日時: 2021 年 6 月 8 日 17:32 UTC
- ARN: arn:aws:iam::aws:policy/AWSDiscoveryContinuousExportFirehosePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSDMSFleetAdvisorServiceRolePolicy

説明: DMS Fleet Advisor がユーザーに代わって CloudWatch メトリクスを管理できるようにします。

AWSDMSFleetAdvisorServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 3 月 6 日 09:10 UTC
- 編集日時: 2023 年 3 月 6 日 09:10 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSDMSFleetAdvisorServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSDMSServerlessServiceRolePolicy

説明: AWS ユーザーに代わってアカウントで DMS リソースを作成および管理するための DMS Serverless アクセス許可を付与します

AWSDMSServerlessServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 5 月 18 日 20:28 UTC
- 編集日時: 2025 年 11 月 5 日 14:19 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSDMSServerlessServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
  "Statement" : [
    {
      "Sid" : "id0",
      "Effect" : "Allow",
      "Action" : [
        "dms:CreateReplicationInstance",
        "dms:CreateReplicationTask"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "dms:req-tag/ResourceCreatedBy" : "DMSServerless"
        }
      }
    },
    {
      "Sid" : "id1",
      "Effect" : "Allow",
      "Action" : [
        "dms:DescribeReplicationInstances",
        "dms:DescribeReplicationTasks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "id2",
      "Effect" : "Allow",
      "Action" : [
        "dms:StartReplicationTask",
        "dms:StopReplicationTask",
        "dms:ModifyReplicationTask",
        "dms:DeleteReplicationTask",
        "dms:ModifyReplicationInstance",
        "dms:DeleteReplicationInstance"
      ],
      "Resource" : [
        "arn:aws:dms:*:*:rep:*",
        "arn:aws:dms:*:*:task:*"
      ],
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "aws:ResourceTag/ResourceCreatedBy" : "DMSServerless"
        }
      }
```

```
    },
    {
      "Sid" : "id3",
      "Effect" : "Allow",
      "Action" : [
        "dms:TestConnection",
        "dms:DeleteConnection"
      ],
      "Resource" : [
        "arn:aws:dms:*:*:rep:*",
        "arn:aws:dms:*:*:endpoint:*"
      ]
    },
    {
      "Sid" : "id4",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:PutObjectTagging"
      ],
      "Resource" : [
        "arn:aws:s3:::dms-serverless-premigration-results-*",
        "arn:aws:s3:::dms-premigration-results-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "id5",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketPolicy",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::dms-serverless-premigration-results-*",
        "arn:aws:s3:::dms-premigration-results-*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "id6",
      "Effect" : "Allow",
      "Action" : [
        "dms:StartReplicationTaskAssessmentRun"
      ],
      "Resource" : [
        "arn:aws:dms:*:*:task:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSEC2CapacityManagerServiceRolePolicy

説明: EC2 Capacity Manager がキャパシティリソースを管理し、ユーザーに代わって AWS Organizations と統合できるようにします。

`AWSEC2CapacityManagerServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2025 年 10 月 9 日 22:04 UTC
- 編集日時: 2025 年 10 月 9 日 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2CapacityManagerServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowOrganizationsDefaultReadActions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:ListChildren",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "AllowOrganizationsListDelegatedAdministratorsAction",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLikeIfExists" : {
          "organizations:ServicePrincipal" : [
            "ec2.capacitymanager.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSEC2CapacityReservationFleetRolePolicy

説明: EC2 CapacityReservation Fleet サービスにキャパシティ予約の管理を許可

AWSEC2CapacityReservationFleetRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 9 月 29 日 14:43 UTC

- 編集日時: 2025 年 3 月 3 日 23:22 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSEC2CapacityReservationFleetRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeInstances"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateCapacityReservation",
        "ec2:CancelCapacityReservation",
        "ec2:ModifyCapacityReservation"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:capacity-reservation/*"
      ],
      "Condition" : {
        "ArnLike" : {
          "ec2:CapacityReservationFleet" : "arn:aws:ec2:*:*:capacity-reservation-fleet/
crf-*"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:capacity-reservation/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateCapacityReservation"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSEC2FleetServiceRolePolicy

説明: EC2 フリートがインスタンスを起動および管理できるようにします。

AWSEC2FleetServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 3 月 21 日 00:08 UTC
- 編集日時: 2020 年 5 月 4 日 20:10 UTC

- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSEC2FleetServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSEC2SpotFleetServiceRolePolicy

説明: EC2 スポットフリートがスポットフリートインスタンスを起動および管理することを許可します

AWSEC2SpotFleetServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 10 月 23 日 19:13 UTC
- 編集日時: 2020 年 3 月 16 日 19:16 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSEC2SpotFleetServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSEC2SpotServiceRolePolicy

説明: EC2 スポットによるスポットインスタンスの起動および管理を許可します

AWSEC2SpotServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 9 月 18 日 18:51 UTC
- 編集日時: 2018 年 12 月 12 日 00:13 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSEC2SpotServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSEC2SqlHaInstancePolicy

説明: ECAmazon EC2インスタンスプロファイルを介してインスタンスの高可用性状態を検出できるようにする Amazon EC2 インスタンスのアクセス許可。 EC2

AWSEC2SqlHaInstancePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSEC2SqlHaInstancePolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 11 月 13 日 01:49 UTC
- 編集日時: 2025 年 11 月 13 日 01:49 UTC
- ARN: arn:aws:iam::aws:policy/AWSEC2SqlHaInstancePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/SqlHaMonitored" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSEc2SqlHa" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
```

```
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2messages:AcknowledgeMessage",
        "ec2messages:DeleteMessage",
        "ec2messages:FailMessage",
        "ec2messages:GetEndpoint",
        "ec2messages:GetMessages",
        "ec2messages:SendReply"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSEC2SqlHaServiceRolePolicy

説明: スタンバイ/パッシブインスタンスを検出するための EC2 SQL High Availability サービスのアクセス許可

`AWSEC2SqlHaServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2025 年 11 月 13 日 01:34 UTC
- 編集日時: 2025 年 11 月 13 日 01:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2SqlHaServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSSMSendCommandToTaggedInstances",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/SqlHaMonitored" : "true"
        }
      }
    },
    {
      "Sid" : "AllowSSMSendCommandOfOwnedDoc",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSEC2-DetectSqlHa*"
```

```
      ]
    },
    {
      "Sid" : "AllowSSMNonMutating",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation",
        "ssm:GetCommandInvocation",
        "ssm:ListCommands",
        "ssm:ListCommandInvocations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowEC2NonMutating",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeTags"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowEventsMutateManagedRule",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:PutRule",
        "events:DeleteRule",
        "events:RemoveTargets"
      ],
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "ec2sqlha.amazonaws.com",
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      },
      "Resource" : "arn:aws:events:*:*:rule/AWSEC2SqlHa*"
    },
    {
      "Sid" : "AllowEventsNonMutatingManagedRule",
      "Effect" : "Allow",
```

```
      "Action" : [
        "events:ListTargetsByRule",
        "events:DescribeRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/AWSEC2SqlHa*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSEC2VssSnapshotPolicy

説明: このポリシーは、Amazon EC2 Windows インスタンスにアタッチされている IAM ロールにアタッチされ、Amazon EC2 VSS ソリューションが Amazon マシンイメージ (AMI) と EBS スナップショットにタグを作成および追加できるようにします。

`AWSEC2VssSnapshotPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSEC2VssSnapshotPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 3 月 27 日 16:32 UTC
- 編集日時: 2024 年 11 月 20 日 17:44 UTC
- ARN: `arn:aws:iam::aws:policy/AWSEC2VssSnapshotPolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeInstanceInfo",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ArnLike" : {
          "ec2:SourceInstanceARN" : "arn:aws:ec2:*:*:instance/${ec2:InstanceId}"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotsWithTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshots"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AwsVssConfig" : "*"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotsAccessInstance",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:CreateSnapshots"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ArnLike" : {
          "ec2:SourceInstanceARN" : "arn:aws:ec2:*:*:instance/${ec2:InstanceId}"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotsAccessVolume",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshots"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "Sid" : "CreateImageWithTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateImage"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:image/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AwsVssConfig" : "*"
        }
      }
    },
    {
      "Sid" : "CreateImageAccessInstance",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateImage"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ArnLike" : {
          "ec2:SourceInstanceARN" : "arn:aws:ec2:*:*:instance/${ec2:InstanceId}"
        }
      }
    },
    {
      "Sid" : "CreateTagsOnResourceCreation",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:image/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateImage",
            "CreateSnapshots"
          ]
        }
      }
    },
    {
      "Sid" : "CreateTagsAfterResourceCreation",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:image/*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/AwsVssConfig" : "*"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AppConsistent",
            "Device"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "DescribeImagesAndSnapshots",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSECRPullThroughCache_ServiceRolePolicy

説明: AWS ECR プルスルーキャッシュによって使用または管理される AWS サービスとリソースへのアクセスを有効にします

AWSECRPullThroughCache_ServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 11 月 26 日 21:51 UTC
- 編集日時: 2025 年 3 月 6 日 21:22 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ECR",
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:InitiateLayerUpload",
        "ecr:UploadLayerPart",
        "ecr:CompleteLayerUpload",
        "ecr:PutImage",
        "ecr:BatchGetImage",
        "ecr:BatchImportUpstreamImage",
        "ecr:GetDownloadUrlForLayer",
        "ecr:GetImageCopyStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManager",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:ecr-pullthroughcache/*",
      "Condition" : {
        "StringEquals" : {
```

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSElasticBeanstalkCustomPlatformforEC2Role

説明: EC2 インスタンスの起動、EBS スナップショットと AMI の作成、Amazon CloudWatch Logs へのログのストリーミング、および Amazon S3 へのアーティファクトの保存を行うためのアクセス許可をカスタムプラットフォームビルダー環境内インスタンスに提供します。

`AWSElasticBeanstalkCustomPlatformforEC2Role` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSElasticBeanstalkCustomPlatformforEC2Role` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 2 月 21 日 22:50 UTC
- 編集日時: 2017 年 2 月 21 日 22:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkCustomPlatformforEC2Role`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSElasticBeanstalkEnhancedHealth

説明: Health Monitoring システムの AWS Elastic Beanstalk サービスポリシー

AWSElasticBeanstalkEnhancedHealth は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElasticBeanstalkEnhancedHealth をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2016 年 2 月 8 日 23:17 UTC
- 編集日時: 2018 年 4 月 9 日 22:12 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkEnhancedHealth

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSElasticBeanstalkMaintenance

説明: AWS Elastic Beanstalk サービスロールポリシーは、メンテナンス目的でユーザーに代わってリソースを更新するための制限付きアクセス許可を付与します。

AWSElasticBeanstalkMaintenance は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 1 月 11 日 23:22 UTC
- 編集日時: 2024 年 4 月 29 日 21:48 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkMaintenance

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy

説明: このポリシーは AWS 、Elastic Beanstalk 環境のマネージド更新を実行するために使用される Elastic Beanstalk サービスロール用です。このポリシーは他のユーザーやロールには適用しないでください。このポリシーは、AutoScaling、EC2、ECS、Elastic Load Balancing、CloudFormation など、さまざまな AWS サービスでリソースを作成および管理するための広範なアクセス許可を付与します。このポリシーでは、それらのサービスで使用可能なすべての IAM ロールを渡すことも許可されます。

`AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 3 月 3 日 22:18 UTC
- 編集日時: 2025 年 2 月 27 日 16:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ElasticBeanstalkPermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticbeanstalk:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowPassRoleToElasticBeanstalkAndDownstreamServices",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "elasticbeanstalk.amazonaws.com",
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn",
```

```
            "autoscaling.amazonaws.com",
            "elasticloadbalancing.amazonaws.com",
            "ecs.amazonaws.com",
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAccountLimits",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeLaunchConfigurations",
        "autoscaling:DescribeLoadBalancers",
        "autoscaling:DescribeNotificationConfigurations",
        "autoscaling:DescribeScalingActivities",
        "autoscaling:DescribeScheduledActions",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "logs:DescribeLogGroups",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeOrderableDBInstanceOptions",
        "sns:ListSubscriptionsByTopic"
```

```
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EC2BroadOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AssociateAddress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions",
        "ec2:DeleteSecurityGroup",
        "ec2:DisassociateAddress",
        "ec2:ReleaseAddress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2RunInstancesOperationPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ec2:LaunchTemplate" : "arn:aws:ec2:*:*:launch-template/*"
        }
      }
    },
    {
      "Sid" : "EC2TerminateInstancesOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
```

```
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" : [
            "arn:aws:cloudformation:*:*:stack/awseb-e-*",
            "arn:aws:cloudformation:*:*:stack/eb-*"
          ]
        }
      }
    },
    {
      "Sid" : "ECSBroadOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecs:CreateCluster",
        "ecs:DescribeClusters",
        "ecs:RegisterTaskDefinition"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ECSDeleteClusterOperationPermissions",
      "Effect" : "Allow",
      "Action" : "ecs:DeleteCluster",
      "Resource" : "arn:aws:ecs:*:*:cluster/awseb-*"
    },
    {
      "Sid" : "ASGOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:AttachInstances",
        "autoscaling:CreateAutoScalingGroup",
        "autoscaling:CreateLaunchConfiguration",
        "autoscaling:CreateOrUpdateTags",
        "autoscaling:DeleteLaunchConfiguration",
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:DeleteScheduledAction",
        "autoscaling:DetachInstances",
        "autoscaling:DeletePolicy",
        "autoscaling:PutScalingPolicy",
        "autoscaling:PutScheduledUpdateGroupAction",
        "autoscaling:PutNotificationConfiguration",
        "autoscaling:ResumeProcesses",
        "autoscaling:SetDesiredCapacity",
        "autoscaling:SuspendProcesses",
```

```
        "autoscaling:TerminateInstanceInAutoScalingGroup",
        "autoscaling:UpdateAutoScalingGroup"
      ],
      "Resource" : [
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/awseb-e-
*",
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/eb-*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/awseb-e-*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/eb-*"
      ]
    },
    {
      "Sid" : "CFNOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:*"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awseb-*",
        "arn:aws:cloudformation:*:*:stack/eb-*"
      ]
    },
    {
      "Sid" : "ELBOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
        "elasticloadbalancing:ConfigureHealthCheck",
        "elasticloadbalancing:CreateLoadBalancer",
        "elasticloadbalancing:DeleteLoadBalancer",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:RegisterTargets"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:targetgroup/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:targetgroup/eb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/eb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/*/awseb-*/*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/*/eb-*/*"
      ]
```

```
    },
    {
      "Sid" : "CWLogsOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:DeleteLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*"
    },
    {
      "Sid" : "S3ObjectOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionAcl",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:PutObjectVersionAcl"
      ],
      "Resource" : "arn:aws:s3:::elasticbeanstalk-*/*"
    },
    {
      "Sid" : "S3BucketOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:GetBucketPolicy",
        "s3:ListBucket",
        "s3:PutBucketPolicy"
      ],
      "Resource" : "arn:aws:s3:::elasticbeanstalk-*"
    },
    {
      "Sid" : "SNSOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:GetTopicAttributes",
        "sns:SetTopicAttributes",
```

```
        "sns:Subscribe"
      ],
      "Resource" : "arn:aws:sns:*:*:ElasticBeanstalkNotifications-*"
    },
    {
      "Sid" : "SQSOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:awseb-e-*",
        "arn:aws:sqs:*:*:eb-*"
      ]
    },
    {
      "Sid" : "CWPutMetricAlarmOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:awseb-*",
        "arn:aws:cloudwatch:*:*:alarm:eb-*"
      ]
    },
    {
      "Sid" : "AllowECSTagResource",
      "Effect" : "Allow",
      "Action" : [
        "ecs:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ecs:CreateAction" : [
            "CreateCluster",
            "RegisterTaskDefinition"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "LaunchTemplateTagPropagationPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:createTags",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateLaunchTemplate",
            "RunInstances"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSElasticBeanstalkManagedUpdatesServiceRolePolicy

説明: マネージド更新に制限されたアクセス許可を付与する AWS Elastic Beanstalk サービスロールポリシー。

AWSElasticBeanstalkManagedUpdatesServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー

- 作成日時: 2019 年 11 月 21 日 22:35 UTC
- 編集日時: 2024 年 4 月 29 日 23:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkManagedUpdatesServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v9 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSElasticBeanstalkMulticontainerDocker

説明: マルチコンテナの Docker 環境内インスタンスに、Amazon EC2 Container Service を使用してコンテナデプロイタスクを管理するためのアクセス権を提供します。

`AWSElasticBeanstalkMulticontainerDocker` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElasticBeanstalkMulticontainerDocker をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2016 年 2 月 8 日 23:15 UTC
- 編集日時: 2023 年 3 月 23 日 22:04 UTC
- ARN: arn:aws:iam::aws:policy/AWSElasticBeanstalkMulticontainerDocker

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSElasticBeanstalkReadOnly

説明: 読み取り専用アクセス許可を付与します。 AWS Elastic Beanstalk アプリケーションに関連するリソースに関する情報を取得するための直接アクセスをオペレーターに明示的に許可します。

`AWSElasticBeanstalkReadOnly` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSElasticBeanstalkReadOnly` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 1 月 22 日 19:02 UTC
- 編集日時: 2021 年 1 月 22 日 19:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkReadOnly`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSElasticBeanstalkRoleCore

説明: AWSElasticBeanstalkRoleCore (Elastic Beanstalk オペレーションロール) であり、ウェブサービス環境のコアオペレーションを許可します。

`AWSElasticBeanstalkRoleCore` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSElasticBeanstalkRoleCore` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 6 月 5 日 21:48 UTC
- 編集日時: 2024 年 4 月 30 日 00:01 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleCore

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSElasticBeanstalkRoleCWL

説明: (Elastic Beanstalk オペレーションロール) 環境が Amazon CloudWatch Logs ロググループを管理できるようにします。

`AWSElasticBeanstalkRoleCWL` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSElasticBeanstalkRoleCWL` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 6 月 5 日 21:49 UTC
- 編集日時: 2020 年 6 月 5 日 21:49 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleCWL`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCWL",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:DeleteLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSElasticBeanstalkRoleECS

説明: (Elastic Beanstalk オペレーションロール) 複数コンテナの Docker 環境で Amazon ECS クラスターを管理できるようにします。

AWSElasticBeanstalkRoleECS は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElasticBeanstalkRoleECS をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 6 月 5 日 21:47 UTC
- 編集日時: 2023 年 3 月 23 日 22:43 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleECS

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSElasticBeanstalkRoleRDS

説明: (Elastic Beanstalk オペレーションロール) 環境で Amazon RDS インスタンスを統合できるようにします。

AWSElasticBeanstalkRoleRDS は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElasticBeanstalkRoleRDS をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 6 月 5 日 21:46 UTC

- 編集日時: 2020 年 6 月 5 日 21:46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleRDS`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSElasticBeanstalkRoleSNS

説明: (Elastic Beanstalk オペレーションロール) 環境で Amazon SNS トピック統合を有効にできるようにします。

AWSElasticBeanstalkRoleSNS は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElasticBeanstalkRoleSNS をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 6 月 5 日 21:46 UTC
- 編集日時: 2020 年 6 月 5 日 21:46 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleSNS

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSElasticBeanstalkRoleWorkerTier

説明: (Elastic Beanstalk オペレーションロール) ワーカー環境階層が Amazon DynamoDB テーブルと Amazon SQS キューを作成できるようにします。

`AWSElasticBeanstalkRoleWorkerTier` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSElasticBeanstalkRoleWorkerTier` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 6 月 5 日 21:43 UTC
- 編集日時: 2020 年 6 月 5 日 21:43 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleWorkerTier`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSElasticBeanstalkService

説明: このポリシーは非推奨化される予定です。ガイダンスについては、https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/iam-servicerole.html. AWS Elastic Beanstalk Service ロールポリシーを参照してください。ロールポリシーは、ユーザーに代わってリソース (AutoScaling、EC2, S3、CloudFormation、ELB など) を作成および管理するためのアクセス許可を付与します。

`AWSElasticBeanstalkService` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSElasticBeanstalkService` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2016 年 4 月 11 日 20:27 UTC
- 編集日時: 2023 年 5 月 10 日 19:29 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkService`

ポリシーのバージョン

ポリシーのバージョン: v17 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSElasticBeanstalkServiceRolePolicy

説明:ユーザーに代わってリソース (AutoScaling、EC2, S3CloudFormation、ELB など) を作成および管理するためのアクセス許可を付与する AWS Elastic Beanstalk サービスにリンクされたロールポリシー。

`AWSElasticBeanstalkServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー

- 作成日時: 2017 年 9 月 13 日 23:46 UTC
- 編集日時: 2019 年 6 月 6 日 21:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSElasticBeanstalkWebTier

説明: ウェブサーバー環境内インスタンスに、Amazon S3 にログファイルをアップロードするためのアクセス権を付与します。

AWSElasticBeanstalkWebTier は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElasticBeanstalkWebTier をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2016 年 2 月 8 日 23:08 UTC
- 編集日時: 2020 年 9 月 9 日 19:38 UTC
- ARN: arn:aws:iam::aws:policy/AWSElasticBeanstalkWebTier

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSElasticBeanstalkWorkerTier

説明: ワーカー環境内インスタンスに、Amazon S3 へのログファイルのアップロード、Amazon SQS によるアプリケーションのジョブキューのモニタリング、Amazon DynamoDB によるリーダー選定の実行、Amazon CloudWatch へのヘルスモニタリングメトリクス公開を行うためのアクセスを付与します。

`AWSElasticBeanstalkWorkerTier` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSElasticBeanstalkWorkerTier` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2016 年 2 月 8 日 23:12 UTC
- 編集日時: 2020 年 9 月 9 日 19:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkWorkerTier`

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する

- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSElasticDisasterRecoveryAgentInstallationPolicy

説明: このポリシーでは、外部サーバーを復旧するために Elastic Disaster Recovery (DRS) AWS で使用される AWS レプリケーションエージェントをインストールできます AWS。このポリシーを AWS 、レプリケーションエージェントのインストールステップで指定した認証情報を持つ IAM ユーザーまたはロールにアタッチします。

`AWSElasticDisasterRecoveryAgentInstallationPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSElasticDisasterRecoveryAgentInstallationPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 11 月 17 日 10:37 UTC
- 編集日時: 2023 年 11 月 27 日 12:38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryAgentInstallationPolicy`

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSElasticDisasterRecoveryAgentPolicy

説明: このポリシーでは、 AWS レプリケーションエージェントの使用を許可します。レプリケーションエージェントは、Elastic Disaster Recovery (DRS) AWS でソースサーバーを復旧するために使用します AWS。IAM ユーザーまたはロールにこのポリシーをアタッチすることはおすすめしません。

AWSElasticDisasterRecoveryAgentPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElasticDisasterRecoveryAgentPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2021 年 11 月 17 日 10:32 UTC
- 編集日時: 2023 年 11 月 27 日 13:44 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryAgentPolicy`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSElasticDisasterRecoveryConsoleFullAccess

説明: このポリシーは、Elastic Disaster Recovery (DRS) のすべてのパブリック APIs AWS へのフルアクセスと、KMS キー、License Manager、Resource Groups、Elastic Load Balancing、IAM、および EC2 情報の読み取り許可を提供します。このポリシーを IAM ユーザーまたはロールにアタッチします。

`AWSElasticDisasterRecoveryConsoleFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSElasticDisasterRecoveryConsoleFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 11 月 17 日 10:46 UTC
- 編集日時: 2025 年 1 月 12 日 07:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryConsoleFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ConsoleFullAccess1",
      "Effect" : "Allow",
      "Action" : [
        "drs:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess2",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeLaunchTemplateVersions",
```

```
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetEbsDefaultKmsKeyId",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeHosts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess4",
      "Effect" : "Allow",
      "Action" : "license-manager:ListLicenseConfigurations",
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess5",
      "Effect" : "Allow",
      "Action" : "resource-groups:ListGroups",
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess6",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DescribeLoadBalancers",
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess7",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListInstanceProfiles",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess8",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
```

```
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryConversionServerRole",
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryRecoveryInstanceRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess9",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess10",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions",
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
```

```
    },
    {
      "Sid" : "ConsoleFullAccess11",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess12",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess13",
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:GetConsoleOutput",
        "ec2:GetConsoleScreenshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
```

```
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess14",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess15",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess16",
      "Effect" : "Allow",
```

```
      "Action" : "ec2:CreateSecurityGroup",
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Sid" : "ConsoleFullAccess17",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess18",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess19",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
```

```
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess20",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess21",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume",
        "ec2:StartInstances",
        "ec2:GetConsoleOutput",
        "ec2:GetConsoleScreenshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AWSDRS" : "AllowLaunchingIntoThisInstance"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "ConsoleFullAccess22",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess23",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess24",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
```

```
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess25",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess26",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateSecurityGroup",
            "CreateVolume",
            "CreateSnapshot",
            "RunInstances"
          ]
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
```

```
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess27",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateLaunchTemplate"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess28",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess29",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess30",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
```

```
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSElasticDisasterRecoveryConsoleFullAccess_v2

説明: このポリシーは、Elastic Disaster Recovery (AWS DRS) のすべてのパブリック APIs と、AWS DRS コンソールで使用される他の AWS サービスのすべてのパブリック APIs AWS へのフルアクセスを提供します。このポリシーをユーザーまたはロールにアタッチします。

`AWSElasticDisasterRecoveryConsoleFullAccess_v2` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSElasticDisasterRecoveryConsoleFullAccess_v2` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 11 月 27 日 13:35 UTC
- 編集日時: 2025 年 7 月 2 日 15:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryConsoleFullAccess_v2`

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ConsoleFullAccess1",
      "Effect" : "Allow",
      "Action" : [
        "drs:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess2",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeLaunchTemplateVersions",
```

```
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetEbsDefaultKmsKeyId",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeHosts",
        "ec2:GetInstanceTypesFromInstanceRequirements"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess4",
      "Effect" : "Allow",
      "Action" : "license-manager:ListLicenseConfigurations",
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess5",
      "Effect" : "Allow",
      "Action" : "resource-groups:ListGroups",
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess6",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DescribeLoadBalancers",
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess7",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListInstanceProfiles",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess8",
      "Effect" : "Allow",
```

```
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryConversionServerRole",
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryRecoveryInstanceRole",
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryRecoveryInstanceWithLaunchActionsRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess9",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess10",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions",
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
```

```
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess11",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess12",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess13",
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:GetConsoleOutput",
        "ec2:GetConsoleScreenshot"
      ],
```

```
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess14",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess15",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
```

```
    {
      "Sid" : "ConsoleFullAccess16",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSecurityGroup",
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Sid" : "ConsoleFullAccess17",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess18",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess19",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
```

```
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess20",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess21",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume",
        "ec2:StartInstances",
        "ec2:GetConsoleOutput",
        "ec2:GetConsoleScreenshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AWSDRS" : "AllowLaunchingIntoThisInstance"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
```

```
            "drs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess22",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess23",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess24",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
```

```
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess25",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess26",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateSecurityGroup",
            "CreateVolume",
            "CreateSnapshot",
            "RunInstances",
```

```
            "CreateNetworkInterface"
          ]
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess27",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateLaunchTemplate"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess28",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess29",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess30",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation",
```

```
        "ssm:DescribeParameters"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess31",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-definition/AWS-CreateImage:$DEFAULT",
        "arn:aws:ssm:*:*:document/AWSMigration-ValidateNetworkConnectivity",
        "arn:aws:ssm:*:*:document/AWSMigration-VerifyMountedVolumes",
        "arn:aws:ssm:*:*:document/AWSMigration-ValidateHttpResponse",
        "arn:aws:ssm:*:*:document/AWSMigration-ValidateDiskSpace",
        "arn:aws:ssm:*:*:document/AWSMigration-VerifyProcessIsRunning",
        "arn:aws:ssm:*:*:document/AWSMigration-LinuxTimeSyncSetting",
        "arn:aws:ssm:*:*:document/AWSEC2-
ApplicationInsightsCloudwatchAgentInstallAndConfigure",
        "arn:aws:ssm:*:*:automation-execution/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess32",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess33",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListDocuments",
        "ssm:ListCommandInvocations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess34",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:PutParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/
ManagedByAWSElasticDisasterRecoveryService-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess35",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ssm:DescribeDocument",
        "ssm:GetDocument"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/*"
    },
    {
      "Sid" : "ConsoleFullAccess36",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameters"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/ManagedByAWSElasticDisasterRecovery-*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess37",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution"
      ],
      "Resource" : "arn:aws:ssm:*:*:automation-execution/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess38",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateIamInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "Null" : {
```

```
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess39",
      "Effect" : "Allow",
      "Action" : "ec2:CreateFleet",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:fleet/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess40",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateFleet"
          ]
        },
        "ForAnyValue:StringEquals" : {
```

```
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess41",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess42",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess43",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
```

```
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "ConsoleFullAccess44",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterfacePermission"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSElasticDisasterRecoveryConversionServerPolicy

説明: このポリシーは、Elastic Disaster Recovery Conversion AWS サーバーのインスタンスロールにアタッチされます。このポリシーにより、Elastic Disaster Recovery (DRS) コンバージョンサーバー (Elastic Disaster Recovery によって起動される EC2 インスタンス) が DRS サービスと通信できるようになります。このポリシーが適用された IAM ロールは DRS によって DRS 変換サーバーに (EC2 インスタンスプロファイルとして) アタッチされます。DRS 変換サーバーは、必要に応じて DRS によって自動的に起動および終了されます。IAM ユーザーまたはロールにこのポリシーをア

タッチすることはおすすめしません。DRS 変換サーバーは、ユーザーが DRS コンソール、CLI、または API を使用してソースサーバーを復元することを選択したときに、Elastic Disaster Recovery によって使用されます。

AWSElasticDisasterRecoveryConversionServerPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElasticDisasterRecoveryConversionServerPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2021 年 11 月 17 日 13:42 UTC
- 編集日時: 2023 年 11 月 27 日 13:13 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryConversionServerPolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSElasticDisasterRecoveryCrossAccountReplicationPolicy

説明: このポリシーにより AWS 、Elastic Disaster Recovery (DRS) はクロスアカウントレプリケーションとクロスアカウントフェイルバックをサポートできます。

`AWSElasticDisasterRecoveryCrossAccountReplicationPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSElasticDisasterRecoveryCrossAccountReplicationPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 5 月 14 日 07:16 UTC
- 編集日時: 2024 年 1 月 17 日 13:19 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSElasticDisasterRecoveryEc2InstancePolicy

説明: このポリシーでは、レプリ AWS ケーションエージェントをインストールして使用することを許可します。レプリケーションエージェントは、Elastic Disaster Recovery (DRS) AWS によって使用され、EC2 (クロスリージョンまたはクロス AZ) で実行されるソースサーバーを復旧します。このポリシーを含む IAM ロールは、EC2 インスタンスに (EC2 インスタンスプロファイルとして) アタッチする必要があります。

`AWSElasticDisasterRecoveryEc2InstancePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSElasticDisasterRecoveryEc2InstancePolicy` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 5 月 26 日 12:30 UTC
- 編集日時: 2023 年 11 月 27 日 13:39 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryEc2InstancePolicy`

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSElasticDisasterRecoveryFailbackInstallationPolicy

説明: IAM アイデンティティに AWSElasticDisasterRecoveryFailbackInstallationPolicy ポリシーをアタッチできます。このポリシーにより、リカバリーインスタンスを元のソースインフラストラクチャにフェールバックするために使用される Elastic Disaster Recovery Failback Client のインストールが可能になります。このポリシーを、Elastic Disaster Recovery Failback Client の実行時に提供した認証情報を持つ IAM ユーザーまたはロールにアタッチしてください。

`AWSElasticDisasterRecoveryFailbackInstallationPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSElasticDisasterRecoveryFailbackInstallationPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 11 月 17 日 11:02 UTC
- 編集日時: 2023 年 11 月 27 日 13:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryFailbackInstallationPolicy`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSElasticDisasterRecoveryFailbackPolicy

説明: このポリシーは、リカバリーインスタンスを元のソースインフラストラクチャにフェイルバックするために使用される Elastic Disaster Recovery フェイルバッククライアントの使用を許可します。IAM ユーザーまたはロールにこのポリシーをアタッチすることはおすすめしません。

AWSElasticDisasterRecoveryFailbackPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElasticDisasterRecoveryFailbackPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2021 年 11 月 17 日 10:41 UTC
- 編集日時: 2023 年 11 月 27 日 12:56 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryFailbackPolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSElasticDisasterRecoveryLaunchActionsPolicy

説明: このポリシーでは、Amazon SSM および追加のサービスに必要なアクセス許可を使用して、Elastic Disaster Recovery (AWS DRS) AWS で起動後のアクションを実行できます。このポリシーを IAM ロールまたはユーザーにアタッチします。

`AWSElasticDisasterRecoveryLaunchActionsPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSElasticDisasterRecoveryLaunchActionsPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 9 月 13 日 07:38 UTC
- 編集日時: 2025 年 7 月 2 日 15:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryLaunchActionsPolicy`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LaunchActionsPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeParameters"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "LaunchActionsPolicy2",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/*",
        "arn:aws:ssm:*:*:automation-definition/*:*",
        "arn:aws:ssm:*:*:automation-execution/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Sid" : "LaunchActionsPolicy3",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*::document/AWS-*",
        "arn:aws:ssm:*::document/AWSCodeDeployAgent-*",
        "arn:aws:ssm:*::document/AWSConfigRemediation-*",
        "arn:aws:ssm:*::document/AWSConformancePacks-*",
        "arn:aws:ssm:*::document/AWSDisasterRecovery-*",
        "arn:aws:ssm:*::document/AWSDistroOTel-*",
        "arn:aws:ssm:*::document/AWSDocs-*",
        "arn:aws:ssm:*::document/AWSEC2-*",
        "arn:aws:ssm:*::document/AWSEC2Launch-*",
        "arn:aws:ssm:*::document/AWSFIS-*",
        "arn:aws:ssm:*::document/AWSFleetManager-*",
        "arn:aws:ssm:*::document/AWSIncidents-*",
        "arn:aws:ssm:*::document/AWSKinesisTap-*",
        "arn:aws:ssm:*::document/AWSMigration-*",
        "arn:aws:ssm:*::document/AWSNVMe-*",
        "arn:aws:ssm:*::document/AWSNitroEnclavesWindows-*",
        "arn:aws:ssm:*::document/AWSObservabilityExporter-*",
        "arn:aws:ssm:*::document/AWSPVDriver-*",
        "arn:aws:ssm:*::document/AWSQuickSetupType-*",
        "arn:aws:ssm:*::document/AWSQuickStarts-*",
        "arn:aws:ssm:*::document/AWSRefactorSpaces-*",
        "arn:aws:ssm:*::document/AWSResilienceHub-*",
        "arn:aws:ssm:*::document/AWSSAP-*",
        "arn:aws:ssm:*::document/AWSSAPTools-*",
        "arn:aws:ssm:*::document/AWSSQLServer-*",
        "arn:aws:ssm:*::document/AWSSSO-*",
        "arn:aws:ssm:*::document/AWSSupport-*",
        "arn:aws:ssm:*::document/AWSSystemsManagerSAP-*",
        "arn:aws:ssm:*::document/AmazonCloudWatch-*",
        "arn:aws:ssm:*::document/AmazonCloudWatchAgent-*",
        "arn:aws:ssm:*::document/AmazonECS-*",
        "arn:aws:ssm:*::document/AmazonEFSUtils-*",
        "arn:aws:ssm:*::document/AmazonEKS-*",
```

```
        "arn:aws:ssm:*::document/AmazonInspector-*",
        "arn:aws:ssm:*::document/AmazonInspector2-*",
        "arn:aws:ssm:*::document/AmazonInternal-*",
        "arn:aws:ssm:*::document/AwsEnaNetworkDriver-*",
        "arn:aws:ssm:*::document/AwsVssComponents-*",
        "arn:aws:ssm:*::automation-definition/AWS-*:*",
        "arn:aws:ssm:*::automation-definition/AWSCodeDeployAgent-*:*",
        "arn:aws:ssm:*::automation-definition/AWSConfigRemediation-*:*",
        "arn:aws:ssm:*::automation-definition/AWSConformancePacks-*:*",
        "arn:aws:ssm:*::automation-definition/AWSDisasterRecovery-*:*",
        "arn:aws:ssm:*::automation-definition/AWSDistroOTel-*:*",
        "arn:aws:ssm:*::automation-definition/AWSDocs-*:*",
        "arn:aws:ssm:*::automation-definition/AWSEC2-*:*",
        "arn:aws:ssm:*::automation-definition/AWSEC2Launch-*:*",
        "arn:aws:ssm:*::automation-definition/AWSFIS-*:*",
        "arn:aws:ssm:*::automation-definition/AWSFleetManager-*:*",
        "arn:aws:ssm:*::automation-definition/AWSIncidents-*:*",
        "arn:aws:ssm:*::automation-definition/AWSKinesisTap-*:*",
        "arn:aws:ssm:*::automation-definition/AWSMigration-*:*",
        "arn:aws:ssm:*::automation-definition/AWSNVMe-*:*",
        "arn:aws:ssm:*::automation-definition/AWSNitroEnclavesWindows-*:*",
        "arn:aws:ssm:*::automation-definition/AWSObservabilityExporter-*:*",
        "arn:aws:ssm:*::automation-definition/AWSPVDriver-*:*",
        "arn:aws:ssm:*::automation-definition/AWSQuickSetupType-*:*",
        "arn:aws:ssm:*::automation-definition/AWSQuickStarts-*:*",
        "arn:aws:ssm:*::automation-definition/AWSRefactorSpaces-*:*",
        "arn:aws:ssm:*::automation-definition/AWSResilienceHub-*:*",
        "arn:aws:ssm:*::automation-definition/AWSSAP-*:*",
        "arn:aws:ssm:*::automation-definition/AWSSAPTools-*:*",
        "arn:aws:ssm:*::automation-definition/AWSSQLServer-*:*",
        "arn:aws:ssm:*::automation-definition/AWSSSO-*:*",
        "arn:aws:ssm:*::automation-definition/AWSSupport-*:*",
        "arn:aws:ssm:*::automation-definition/AWSSystemsManagerSAP-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonCloudWatch-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonCloudWatchAgent-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonECS-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonEFSUtils-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonEKS-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonInspector-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonInspector2-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonInternal-*:*",
        "arn:aws:ssm:*::automation-definition/AwsEnaNetworkDriver-*:*",
        "arn:aws:ssm:*::automation-definition/AwsVssComponents-*:*",
        "arn:aws:ssm:*:*:automation-execution/*"
```

```
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "LaunchActionsPolicy4",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "LaunchActionsPolicy5",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSDRS" : "AllowLaunchingIntoThisInstance"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
```

```
            "drs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "LaunchActionsPolicy6",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListDocuments",
        "ssm:ListCommandInvocations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LaunchActionsPolicy7",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListDocumentVersions",
        "ssm:GetDocument",
        "ssm:DescribeDocument"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/*"
    },
    {
      "Sid" : "LaunchActionsPolicy8",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution"
      ],
      "Resource" : "arn:aws:ssm:*:*:automation-execution/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "LaunchActionsPolicy9",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameters"
      ],
```

```
      "Resource" : "arn:aws:ssm:*:*:parameter/
ManagedByAWSElasticDisasterRecoveryService-*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "LaunchActionsPolicy10",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:PutParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/
ManagedByAWSElasticDisasterRecoveryService-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "LaunchActionsPolicy11",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryRecoveryInstanceWithLaunchActionsRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "drs.amazonaws.com"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSElasticDisasterRecoveryNetworkReplicationPolicy

説明: このポリシーは、Elastic Disaster Recovery (DRS) AWS がネットワークレプリケーションをサポートすることを許可します。

`AWSElasticDisasterRecoveryNetworkReplicationPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSElasticDisasterRecoveryNetworkReplicationPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 6 月 11 日 12:36 UTC
- 編集日時: 2024 年 1 月 2 日 13:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryNetworkReplicationPolicy`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSElasticDisasterRecoveryReadOnlyAccess

説明: IAM アイデンティティに AWSElasticDisasterRecoveryReadOnlyAccess ポリシーをアタッチできます。このポリシーは、Elastic Disaster Recovery (DRS) のすべての読み取り専用パブリック

APIs と、DRS コンソールの完全な読み取り専用使用に必要な他の AWS サービスの一部の読み取り専用 APIs へのアクセス許可を提供します。このポリシーを IAM ユーザーまたはロールにアタッチします。

AWSElasticDisasterRecoveryReadOnlyAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElasticDisasterRecoveryReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 11 月 17 日 10:50 UTC
- 編集日時: 2024 年 7 月 29 日 19:39 UTC
- ARN: arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSReadOnlyAccess1",
      "Effect" : "Allow",
      "Action" : [
        "drs:DescribeJobLogItems",
        "drs:DescribeJobs",
        "drs:DescribeRecoveryInstances",
        "drs:DescribeRecoverySnapshots",
        "drs:DescribeReplicationConfigurationTemplates",
```

```
        "drs:DescribeSourceServers",
        "drs:GetFailbackReplicationConfiguration",
        "drs:GetLaunchConfiguration",
        "drs:GetReplicationConfiguration",
        "drs:ListExtensibleSourceServers",
        "drs:ListStagingAccounts",
        "drs:ListTagsForResource",
        "drs:ListLaunchActions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSReadOnlyAccess2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:GetInstanceTypesFromInstanceRequirements"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSReadOnlyAccess4",
      "Effect" : "Allow",
      "Action" : "iam:ListRoles",
      "Resource" : "*"
    },
    {
      "Sid" : "DRSReadOnlyAccess5",
      "Effect" : "Allow",
      "Action" : "ssm:ListCommandInvocations",
      "Resource" : "*"
    },
    {
      "Sid" : "DRSReadOnlyAccess6",
      "Effect" : "Allow",
      "Action" : "ssm:GetParameter",
      "Resource" : "arn:aws:ssm:*:*:parameter/ManagedByAWSElasticDisasterRecovery-*"
    },
    {
      "Sid" : "DRSReadOnlyAccess7",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ssm:DescribeDocument",
        "ssm:GetDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-CreateImage",
        "arn:aws:ssm:*:*:document/AWSMigration-ValidateNetworkConnectivity",
        "arn:aws:ssm:*:*:document/AWSMigration-VerifyMountedVolumes",
        "arn:aws:ssm:*:*:document/AWSMigration-ValidateHttpResponse",
        "arn:aws:ssm:*:*:document/AWSMigration-ValidateDiskSpace",
        "arn:aws:ssm:*:*:document/AWSMigration-VerifyProcessIsRunning",
        "arn:aws:ssm:*:*:document/AWSMigration-LinuxTimeSyncSetting",
        "arn:aws:ssm:*:*:document/AWSEC2-
ApplicationInsightsCloudwatchAgentInstallAndConfigure"
      ]
    },
    {
      "Sid" : "DRSReadOnlyAccess8",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution"
      ],
      "Resource" : "arn:aws:ssm:*:*:automation-execution/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSElasticDisasterRecoveryRecoveryInstancePolicy

説明: このポリシーは、Elastic Disaster Recovery の Recovery インスタンスのインスタンスロールにアタッチされています。このポリシーにより、Elastic Disaster Recovery によって起動された EC2 インスタンスである Elastic Disaster Recovery (DRS) Recovery インスタンスが DRS サービスと通信し、元のソースインフラストラクチャにフェイルバックできるようになります。このポリシーが適用された IAM ロールは、Elastic Disaster Recovery によって DRS Recovery インスタンスに (EC2 インスタンスプロファイルとして) アタッチされます。IAM ユーザーまたはロールにこのポリシーをアタッチすることはおすすめしません。

`AWSElasticDisasterRecoveryRecoveryInstancePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSElasticDisasterRecoveryRecoveryInstancePolicy` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2021 年 11 月 17 日 10:20 UTC
- 編集日時: 2023 年 11 月 27 日 13:11 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryRecoveryInstancePolicy`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSElasticDisasterRecoveryReplicationServerPolicy

説明: このポリシーは、Elastic Disaster Recovery Replication サーバーのインスタンスロールにアタッチされています。このポリシーは、Elastic Disaster Recovery によって起動された EC2 インスタンスである Elastic Disaster Recovery (DRS) レプリケーションサーバーが DRS サービスと通信し、 AWS アカウントに EBS スナップショットを作成することを許可します。このポリシーが適用された IAM ロールは Elastic Disaster Recovery によって DRS レプリケーションサーバーに (EC2 インスタンスプロファイルとして) アタッチされます。必要に応じて DRS によって自動的に起動および終了されます。DRS レプリケーションサーバーは、DRS によって管理される復旧プロセスの一環として AWS、外部サーバーから へのデータレプリケーションを容易にするために使用されます。IAM ユーザーまたはロールにこのポリシーをアタッチすることはおすすめしません。

AWSElasticDisasterRecoveryReplicationServerPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに
AWSElasticDisasterRecoveryReplicationServerPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2021 年 11 月 17 日 13:34 UTC
- 編集日時: 2023 年 11 月 27 日 13:28 UTC
- ARN: arn:aws:iam::aws:policy/service-role/
  AWSElasticDisasterRecoveryReplicationServerPolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSElasticDisasterRecoveryServiceRolePolicy

説明: このポリシーは、Elastic Disaster Recovery がユーザーに代わって AWS リソースを管理することを許可します。

AWSElasticDisasterRecoveryServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 11 月 17 日 10:56 UTC
- 編集日時: 2025 年 1 月 5 日 14:07 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSElasticDisasterRecoveryServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSServiceRolePolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSServiceRolePolicy2",
      "Effect" : "Allow",
```

```
      "Action" : [
        "drs:TagResource"
      ],
      "Resource" : "arn:aws:drs:*:*:recovery-instance/*"
    },
    {
      "Sid" : "DRSServiceRolePolicy3",
      "Effect" : "Allow",
      "Action" : [
        "drs:CreateRecoveryInstanceForDrs",
        "drs:TagResource"
      ],
      "Resource" : "arn:aws:drs:*:*:source-server/*"
    },
    {
      "Sid" : "DRSServiceRolePolicy4",
      "Effect" : "Allow",
      "Action" : "iam:GetInstanceProfile",
      "Resource" : "*"
    },
    {
      "Sid" : "DRSServiceRolePolicy5",
      "Effect" : "Allow",
      "Action" : "kms:ListRetirableGrants",
      "Resource" : "*"
    },
    {
      "Sid" : "DRSServiceRolePolicy6",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumeAttribute",
```

```
        "ec2:GetEbsDefaultKmsKeyId",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeRouteTables",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeManagedPrefixLists",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetManagedPrefixListAssociations",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSServiceRolePolicy7",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RegisterImage"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSServiceRolePolicy8",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeregisterImage"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy9",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
```

```
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy10",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy11",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume",
        "ec2:ModifyVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy12",
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:GetConsoleOutput",
```

```
        "ec2:GetConsoleScreenshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy13",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy14",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy15",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
```

```
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy16",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Sid" : "DRSServiceRolePolicy17",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy18",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy19",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy20",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy21",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy22",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*"
    },
```

```
    {
      "Sid" : "DRSServiceRolePolicy23",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy24",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ]
    },
    {
      "Sid" : "DRSServiceRolePolicy25",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryReplicationServerRole",
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryConversionServerRole",
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryRecoveryInstanceRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
```

```
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy26",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateLaunchTemplate",
            "CreateSecurityGroup",
            "CreateVolume",
            "CreateSnapshot",
            "RunInstances",
            "CreateNetworkInterface"
          ]
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy27",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:image/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy28",
      "Effect" : "Allow",
      "Action" : "cloudwatch:GetMetricData",
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "DRSServiceRolePolicy29",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy30",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy31",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "DRSServiceRolePolicy32",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterfacePermission",
```

```
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy33",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSElasticDisasterRecoveryStagingAccountPolicy

説明: このポリシーは、ソースサーバーやジョブなどの AWS Elastic Disaster Recovery (DRS) リソースへの読み取り専用アクセスを許可します。また、変換されたスナップショットを作成し、その EBS スナップショットを特定のアカウントと共有することもできます。

AWSElasticDisasterRecoveryStagingAccountPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElasticDisasterRecoveryStagingAccountPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 5 月 26 日 09:49 UTC
- 編集日時: 2023 年 11 月 27 日 13:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryStagingAccountPolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSElasticDisasterRecoveryStagingAccountPolicy_v2

説明: このポリシーは、Elastic Disaster Recovery (DRS) AWS がソースサーバーを別のターゲットアカウントに復旧し、フェイルバックを許可するために使用されます。IAM ユーザーまたはロールにこのポリシーをアタッチすることはおすすめしません。

`AWSElasticDisasterRecoveryStagingAccountPolicy_v2` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSElasticDisasterRecoveryStagingAccountPolicy_v2` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー

- 作成日時: 2023 年 1 月 5 日 12:11 UTC
- 編集日時: 2023 年 11 月 27 日 13:32 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryStagingAccountPolicy_v2

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSElasticLoadBalancingClassicServiceRolePolicy

説明: AWS Elastic Load Balancing コントロールプレーンのサービスリンクロールポリシー - Classic

AWSElasticLoadBalancingClassicServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー

- 作成日時: 2017 年 9 月 19 日 22:36 UTC
- 編集日時: 2019 年 10 月 7 日 23:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticLoadBalancingClassicServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSElasticLoadBalancingServiceRolePolicy

説明: AWS Elastic Load Balancing コントロールプレーンのサービスリンクロールポリシー

AWSElasticLoadBalancingServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 9 月 19 日 22:19 UTC
- 編集日時: 2025 年 11 月 17 日 21:34 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSElasticLoadBalancingServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v10 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAddresses",
        "ec2:DescribeCoipPools",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeVpcClassicLink",
        "ec2:CreateSecurityGroup",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:GetCoipPoolUsage",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:AllocateAddress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:AttachNetworkInterface",
        "ec2:DetachNetworkInterface",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssignIpv6Addresses",
        "ec2:ReleaseAddress",
        "ec2:UnassignIpv6Addresses",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeAvailabilityZones",
        "ec2:AllocateIpamPoolCidr",
        "logs:CreateLogDelivery",
```

```
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries",
        "outposts:GetOutpostInstanceTypes"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSElementalMediaConnectFullAccess

説明: Elemental MediaConnect AWS リソースへのフルアクセスを提供します。

`AWSElementalMediaConnectFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSElementalMediaConnectFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 2 月 12 日 20:07 UTC
- 編集日時: 2025 年 2 月 12 日 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConnectFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSElementalMediaConnectReadOnlyAccess

説明: Elemental MediaConnect AWS リソースへの読み取り専用アクセスを提供します。

`AWSElementalMediaConnectReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSElementalMediaConnectReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 2 月 12 日 20:07 UTC
- 編集日時: 2025 年 2 月 12 日 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConnectReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mediaconnect:ListBridges",
        "mediaconnect:ListEntitlements",
        "mediaconnect:ListFlows",
        "mediaconnect:ListGatewayInstances",
        "mediaconnect:ListGateways",
        "mediaconnect:ListOfferings",
        "mediaconnect:ListReservations",
        "mediaconnect:DescribeBridge",
        "mediaconnect:DescribeFlow",
        "mediaconnect:DescribeFlowSourceMetadata",
        "mediaconnect:DescribeFlowSourceThumbnail",
        "mediaconnect:DescribeGateway",
        "mediaconnect:DescribeGatewayInstance",
        "mediaconnect:DescribeOffering",
        "mediaconnect:DescribeReservation",
        "mediaconnect:ListTagsForResource"
      ],
```

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSElementalMediaConvertFullAccess

説明: AWS マネジメントコンソール および SDK 経由で AWS Elemental MediaConvert へのフルアクセスを提供します。

`AWSElementalMediaConvertFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSElementalMediaConvertFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 6 月 25 日 19:25 UTC
- 編集日時: 2019 年 6 月 10 日 22:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConvertFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSElementalMediaConvertReadOnly

説明: AWS マネジメントコンソール および SDK 経由で AWS Elemental MediaConvert への読み取り専用アクセスを提供します。

AWSElementalMediaConvertReadOnly は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElementalMediaConvertReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 6 月 25 日 19:25 UTC
- 編集日時: 2019 年 6 月 10 日 22:52 UTC
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaConvertReadOnly

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mediaconvert:Get*",
        "mediaconvert:List*",
        "mediaconvert:DescribeEndpoints",
```

```
        "s3:ListAllMyBuckets",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSElementalMediaLiveFullAccess

説明: Elemental MediaLive AWS リソースへのフルアクセスを提供します

`AWSElementalMediaLiveFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSElementalMediaLiveFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 7 月 8 日 17:07 UTC
- 編集日時: 2020 年 7 月 8 日 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaLiveFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSElementalMediaLiveReadOnly

説明: Elemental MediaLive AWS リソースへの読み取り専用アクセスを提供します

`AWSElementalMediaLiveReadOnly` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSElementalMediaLiveReadOnly` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 7 月 8 日 16:38 UTC
- 編集日時: 2024 年 7 月 22 日 17:08 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaLiveReadOnly`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSElementalMediaPackageFullAccess

説明: Elemental MediaPackage AWS リソースへのフルアクセスを提供します

AWSElementalMediaPackageFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElementalMediaPackageFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 12 月 29 日 23:39 UTC
- 編集日時: 2017 年 12 月 29 日 23:39 UTC
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaPackageFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSElementalMediaPackageReadOnly

説明: Elemental MediaPackage AWS リソースへの読み取り専用アクセスを提供します

AWSElementalMediaPackageReadOnly は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElementalMediaPackageReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 12 月 30 日 00:04 UTC
- 編集日時: 2017 年 12 月 30 日 00:04 UTC
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaPackageReadOnly

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSElementalMediaPackageV2FullAccess

説明: Elemental MediaPackageV2 AWS リソースへのフルアクセスを提供します。

`AWSElementalMediaPackageV2FullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSElementalMediaPackageV2FullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 7 月 25 日 20:29 UTC
- 編集日時: 2023 年 7 月 25 日 20:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageV2FullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : "mediapackagev2:*",
    "Resource" : "*"
  }
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSElementalMediaPackageV2ReadOnly

説明: Elemental MediaPackageV2 AWS リソースへの読み取り専用アクセスを提供します。

`AWSElementalMediaPackageV2ReadOnly` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSElementalMediaPackageV2ReadOnly` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 7 月 25 日 20:31 UTC
- 編集日時: 2023 年 7 月 25 日 20:31 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageV2ReadOnly`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "mediapackagev2:List*",
      "mediapackagev2:Get*"
    ],
    "Resource" : "*"
  }
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSElementalMediaStoreFullAccess

説明: すべての MediaStore API への読み取りおよび書き込みのフルアクセスを提供します

`AWSElementalMediaStoreFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSElementalMediaStoreFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2018 年 3 月 5 日 23:15 UTC
- 編集日時: 2018 年 3 月 5 日 23:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaStoreFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mediastore:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:SecureTransport" : "true"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSElementalMediaStoreReadOnly

説明: MediaStore API に対する読み取り専用のアクセス許可を付与

AWSElementalMediaStoreReadOnly は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElementalMediaStoreReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 3 月 8 日 19:48 UTC
- 編集日時: 2018 年 3 月 8 日 19:48 UTC
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaStoreReadOnly

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
        "Bool" : {
          "aws:SecureTransport" : "true"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSElementalMediaTailorFullAccess

説明: Elemental MediaTailor AWS リソースへのフルアクセスを提供します

`AWSElementalMediaTailorFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSElementalMediaTailorFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 11 月 23 日 00:04 UTC
- 編集日時: 2021 年 11 月 23 日 00:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaTailorFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSElementalMediaTailorReadOnly

説明: Elemental MediaTailor AWS リソースへの読み取り専用アクセスを提供します

`AWSElementalMediaTailorReadOnly` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSElementalMediaTailorReadOnly` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 11 月 23 日 00:05 UTC

- 編集日時: 2021 年 11 月 23 日 00:05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaTailorReadOnly`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSEnhancedClassicNetworkingMangementPolicy

説明: 拡張クラシックネットワーク管理機能を有効にするポリシー。

`AWSEnhancedClassicNetworkingMangementPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 9 月 20 日 17:29 UTC
- 編集日時: 2017 年 9 月 20 日 17:29 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEnhancedClassicNetworkingMangementPolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSEntityResolutionConsoleFullAccess

説明: AWS エンティティ解決および関連サービスへのフルアクセスをコンソールに提供します。

AWSEntityResolutionConsoleFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSEntityResolutionConsoleFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 8 月 17 日 17:54 UTC
- 編集日時: 2025 年 12 月 15 日 21:19 UTC
- ARN: arn:aws:iam::aws:policy/AWSEntityResolutionConsoleFullAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
      "Effect" : "Allow",
      "Action" : [
        "entityresolution:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueSourcesConsoleDisplay",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetSchema",
        "glue:SearchTables",
        "glue:GetSchemaByDefinition",
        "glue:GetSchemaVersion",
        "glue:GetSchemaVersionsDiff",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetTableVersion",
        "glue:GetTableVersions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3BucketsConsoleDisplay",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3SourcesConsoleDisplay",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:ListBucketVersions",
        "s3:GetBucketVersioning"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "TaggingConsoleDisplay",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetTagKeys",
        "tag:GetTagValues"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSConsoleDisplay",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListRolesToPickRoleForPassing",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassRoleToEntityResolutionService",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*entityresolution*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "entityresolution.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ManageEventBridgeRules",
      "Effect" : "Allow",
      "Action" : [
```

```
        "events:DeleteRule",
        "events:PutTargets",
        "events:PutRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/entity-resolution-automatic*"
      ]
    },
    {
      "Sid" : "ADXReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:GetDataSet"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CustomerProfilesIntegrationReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "connect:ListInstances",
        "profile:ListDomains",
        "profile:GetDomain",
        "profile:ListIntegrations",
        "profile:ListAccountIntegrations",
        "profile:ListProfileObjectTypes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CustomerProfilesIntegrationWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "profile:PutProfileObjectType"
      ],
      "Resource" : [
        "arn:aws:profile:*:*:domains/*/object-types/*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSEntityResolutionConsoleReadOnlyAccess

説明: 経由で AWS エンティティ解決への読み取り専用アクセスを提供します AWS マネジメントコンソール。

`AWSEntityResolutionConsoleReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSEntityResolutionConsoleReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 8 月 17 日 18:18 UTC
- 編集日時: 2023 年 8 月 17 日 18:18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSEntityResolutionConsoleReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
```

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSFaultInjectionSimulatorEC2Access

説明: このポリシーは、EC2 およびその他の必要なサービスで FIS アクションを実行するためのアクセス許可を Fault Injection Simulator サービスに付与します。

`AWSFaultInjectionSimulatorEC2Access` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSFaultInjectionSimulatorEC2Access` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 10 月 26 日 20:39 UTC
- 編集日時: 2025 年 11 月 11 日 09:49 UTC

- ARN: arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorEC2Access

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowEc2Actions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RebootInstances",
        "ec2:SendSpotInstanceInterruptions",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Sid" : "AllowEc2InstancesWithEncryptedEbsVolumes",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : [
        "arn:aws:kms:*:*:key/*"
      ],
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com"
        },
        "Bool" : {
```

```
          "kms:GrantIsForAWSResource" : "true"
        }
      }
    },
    {
      "Sid" : "AllowSSMSendOnEc2",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:document/*"
      ]
    },
    {
      "Sid" : "AllowSSMStopOnEc2",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CancelCommand",
        "ssm:ListCommands"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeInstances",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeInstances",
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeSubnets",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeSubnets",
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSFaultInjectionSimulatorECSAccess

説明: このポリシーは、Fault Injection Simulator サービスに、ECS およびその他の必要なサービスで FIS アクションを実行する許可を付与します。

`AWSFaultInjectionSimulatorECSAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSFaultInjectionSimulatorECSAccess` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 10 月 26 日 20:37 UTC
- 編集日時: 2025 年 11 月 11 日 09:49 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorECSAccess`

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeClusters",
        "ecs:ListContainerInstances"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:cluster/*"
      ]
    },
    {
      "Sid" : "Tasks",
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeTasks",
        "ecs:StopTask"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:task/*/*"
      ]
    },
    {
      "Sid" : "ContainerInstances",
      "Effect" : "Allow",
      "Action" : [
        "ecs:UpdateContainerInstancesState"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:container-instance/*/*"
      ]
    },
    {
      "Sid" : "ListTasks",
      "Effect" : "Allow",
      "Action" : [
        "ecs:ListTasks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMSend",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ssm:*:*:managed-instance/*",
```

```
        "arn:aws:ssm:*:*:document/*"
      ]
    },
    {
      "Sid" : "SSMList",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListCommands",
        "ssm:CancelCommand"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TargetResolutionByTags",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeContainerInstances",
      "Effect" : "Allow",
      "Action" : "ecs:DescribeContainerInstances",
      "Resource" : "arn:aws:ecs:*:*:container-instance/*/*"
    },
    {
      "Sid" : "DescribeInstances",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeInstances",
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeSubnets",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeSubnets",
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSFaultInjectionSimulatorEKSAccess

説明: このポリシーは、Fault Injection Simulator サービスに、EKS およびその他の必要なサービスで FIS アクションを実行する許可を付与します。

`AWSFaultInjectionSimulatorEKSAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSFaultInjectionSimulatorEKSAccess` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 10 月 26 日 20:34 UTC
- 編集日時: 2025 年 3 月 11 日 14:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorEKSAccess`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSFaultInjectionSimulatorNetworkAccess

説明: EC2 ネットワーキングおよびその他の必要なサービスで FIS アクションを実行するためのアクセス許可を付与します。

`AWSFaultInjectionSimulatorNetworkAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSFaultInjectionSimulatorNetworkAccess` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 10 月 26 日 20:32 UTC
- 編集日時: 2025 年 3 月 11 日 13:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorNetworkAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSFaultInjectionSimulatorRDSAccess

説明: このポリシーは、Fault Injection Simulator サービスに、RDS およびその他の FIS アクションを実行するために必要なサービスへのアクセスを付与します。

AWSFaultInjectionSimulatorRDSAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSFaultInjectionSimulatorRDSAccess をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 10 月 26 日 20:30 UTC
- 編集日時: 2025 年 3 月 18 日 15:07 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorRDSAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSFaultInjectionSimulatorSSMAccess

説明: このポリシーは、Fault Injection Simulator サービスに、FIS アクション実行のために必要な SSM およびその他のサービスへのアクセスを付与します。

`AWSFaultInjectionSimulatorSSMAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSFaultInjectionSimulatorSSMAccess` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 10 月 26 日 15:33 UTC
- 編集日時: 2025 年 6 月 25 日 14:22 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorSSMAccess`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/*",
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:automation-definition/*:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution",
        "ssm:StopAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-execution/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:document/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListCommands",
        "ssm:CancelCommand"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSFinSpaceServiceRolePolicy

説明: Amazon FinSpace が使用または管理する AWS のサービス およびリソースへのアクセスを有効にするポリシー

`AWSFinSpaceServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 5 月 12 日 16:42 UTC
- 編集日時: 2023 年 12 月 1 日 21:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSFinSpaceServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSFMAdminFullAccess

説明: FM AWS 管理者のフルアクセス

AWSFMAdminFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSFMAdminFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 5 月 9 日 18:06 UTC
- 編集日時: 2022 年 10 月 20 日 23:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSFMAdminFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSFMAdminReadOnlyAccess

説明: FM AWS オペレーションのモニタリングを許可する FM AWS 管理者の読み取り専用アクセス

`AWSFMAdminReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSFMAdminReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 5 月 9 日 20:07 UTC
- 編集日時: 2022 年 10 月 31 日 22:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSFMAdminReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSFMMemberReadOnlyAccess

説明: AWS Firewall Manager メンバーアカウントの AWS WAF アクションへの読み取り専用アクセスを提供します

`AWSFMMemberReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSFMMemberReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 5 月 9 日 21:05 UTC
- 編集日時: 2018 年 5 月 9 日 21:05 UTC
- ARN: arn:aws:iam::aws:policy/AWSFMMemberReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "fms:GetAdminAccount",
        "waf:Get*",
        "waf:List*",
        "waf-regional:Get*",
        "waf-regional:List*",
        "organizations:DescribeOrganization"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSForWordPressPluginPolicy

説明: AWS for Wordpress プラグインの管理ポリシー

`AWSForWordPressPluginPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSForWordPressPluginPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 10 月 30 日 00:27 UTC
- 編集日時: 2020 年 1 月 20 日 23:20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSForWordPressPluginPolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSGitSyncServiceRolePolicy

説明: AWS Code Connections が git リポジトリからコンテンツを同期できるようにするポリシー

`AWSGitSyncServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 11 月 16 日 17:05 UTC
- 編集日時: 2024 年 4 月 26 日 18:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSGitSyncServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSGlobalAcceleratorSLRPolicy

説明: EC2 Elastic Network Interface とセキュリティグループを管理するためのアクセス許可を AWS Global Accelerator に付与するポリシー。

`AWSGlobalAcceleratorSLRPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 4 月 5 日 19:39 UTC
- 編集日時: 2024 年 10 月 29 日 18:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSGlobalAcceleratorSLRPolicy`

ポリシーのバージョン

ポリシーのバージョン: v9 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2Action1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSubnets",
        "ec2:DescribeRegions",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeAddresses"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2Action2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup",
        "ec2:AssignIpv6Addresses",
        "ec2:UnassignIpv6Addresses"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AWSServiceName" : "GlobalAccelerator"
        }
      }
    },
    {
      "Sid" : "EC2Action3",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "ec2:GetSecurityGroupsForVpc"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ElbAction1",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeTargetGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2Action4",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSGlueConsoleFullAccess

説明: を介して Glue AWS へのフルアクセスを提供します AWS マネジメントコンソール

`AWSGlueConsoleFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSGlueConsoleFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 8 月 14 日 13:37 UTC
- 編集日時: 2023 年 7 月 14 日 14:37 UTC
- ARN: arn:aws:iam::aws:policy/AWSGlueConsoleFullAccess

ポリシーのバージョン

ポリシーのバージョン: v14 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSGlueConsoleSageMakerNotebookFullAccess

説明: 経由で AWS Glue へのフルアクセス AWS マネジメントコンソール と sagemaker ノートブックインスタンスへのアクセスを提供します。

`AWSGlueConsoleSageMakerNotebookFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSGlueConsoleSageMakerNotebookFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 10 月 5 日 17:52 UTC
- 編集日時: 2021 年 7 月 15 日 15:24 UTC
- ARN: arn:aws:iam::aws:policy/AWSGlueConsoleSageMakerNotebookFullAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AwsGlueDataBrewFullAccessPolicy

説明: 経由で AWS Glue DataBrew へのフルアクセスを提供します AWS マネジメントコンソール。また、関連サービス (S3、KMS、Glue など) への特定のアクセスも提供します。

AwsGlueDataBrewFullAccessPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AwsGlueDataBrewFullAccessPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 11 月 11 日 16:51 UTC
- 編集日時: 2022 年 2 月 4 日 18:28 UTC
- ARN: arn:aws:iam::aws:policy/AwsGlueDataBrewFullAccessPolicy

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSGlueDataBrewServiceRole

説明: このポリシーは、ユーザーの Glue データカタログでアクションを実行するためのアクセス許可を Glue に付与します。また、このポリシーは、Glue が VPC 内のリソースに接続するための ENI を作成できるよう ec2 アクションの許可を付与するとともに、Glue による lakeformation の登録データへのアクセスとユーザー Cloudwatch へのアクセス許可も付与します。

AWSGlueDataBrewServiceRole は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSGlueDataBrewServiceRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 12 月 4 日 21:26 UTC
- 編集日時: 2024 年 3 月 20 日 23:28 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSGlueDataBrewServiceRole

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSGlueSchemaRegistryFullAccess

説明: Glue Schema Registry Service AWS へのフルアクセスを提供します

`AWSGlueSchemaRegistryFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSGlueSchemaRegistryFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 11 月 20 日 00:19 UTC
- 編集日時: 2020 年 11 月 20 日 00:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGlueSchemaRegistryFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSGlueSchemaRegistryReadonlyAccess

説明: Glue Schema Registry Service AWS への読み取り専用アクセスを提供します

`AWSGlueSchemaRegistryReadonlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSGlueSchemaRegistryReadonlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 11 月 20 日 00:20 UTC
- 編集日時: 2020 年 11 月 20 日 00:20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGlueSchemaRegistryReadonlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSGlueServiceNotebookRole

説明: AWS お客様がノートブックサーバーを管理できるようにする Glue サービスロールのポリシー

AWSGlueServiceNotebookRole は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSGlueServiceNotebookRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2017 年 8 月 14 日 13:37 UTC
- 編集日時: 2023 年 10 月 9 日 15:59 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSGlueServiceNotebookRole

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSGlueServiceRole

説明: EC2 AWS 、S3、Cloudwatch Logs などの関連サービスへのアクセスを許可する Glue サービスロールのポリシー EC2, S3

`AWSGlueServiceRole` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSGlueServiceRole` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2017 年 8 月 14 日 13:37 UTC
- 編集日時: 2023 年 9 月 11 日 16:39 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSGlueServiceRole`

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AwsGlueSessionUserRestrictedNotebookPolicy

説明: ユーザー自身に関連付けられているノートブックセッションのみを作成および使用できるようにするアクセス許可を提供します。このポリシーには、ユーザーが制限付き Glue セッションロールを渡すことを明示的に許可するアクセス許可も含まれます。

`AwsGlueSessionUserRestrictedNotebookPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AwsGlueSessionUserRestrictedNotebookPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 4 月 18 日 15:24 UTC
- 編集日時: 2024 年 8 月 15 日 20:51 UTC
- ARN: `arn:aws:iam::aws:policy/AwsGlueSessionUserRestrictedNotebookPolicy`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "NotebokAllowActions0",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/owner" : "${aws:PrincipalTag/owner}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
    {
      "Sid" : "AllowGlueTaggingAction",
      "Effect" : "Allow",
      "Action" : [
        "glue:TagResource"
      ],
      "Resource" : "arn:aws:glue:*:*:session/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/owner" : "${aws:PrincipalTag/owner}",
          "aws:RequestTag/owner" : "${aws:PrincipalTag/owner}"
        }
      }
    },
    {
      "Sid" : "NotebookAllowActions1",
      "Effect" : "Allow",
      "Action" : [
```

```
        "glue:StartCompletion",
        "glue:GetCompletion"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:completion/*"
      ]
    },
    {
      "Sid" : "NotebookAllowActions2",
      "Effect" : "Allow",
      "Action" : [
        "glue:RunStatement",
        "glue:GetStatement",
        "glue:ListStatements",
        "glue:CancelStatement",
        "glue:StopSession",
        "glue:DeleteSession",
        "glue:GetSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/owner" : "${aws:PrincipalTag/owner}"
        }
      }
    },
    {
      "Sid" : "NotebookAllowActions3",
      "Effect" : "Allow",
      "Action" : [
        "glue:ListSessions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "NotebookDenyActions",
      "Effect" : "Deny",
      "Action" : [
        "glue:UntagResource",
        "tag:TagResources",
```

```
        "tag:UntagResources"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
    {
      "Sid" : "NotebookPassRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AwsGlueSessionServiceRoleUserRestrictedForNotebook*",
        "arn:aws:iam::*:role/AwsGlueSessionUserRestrictedNotebookServiceRole*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AwsGlueSessionUserRestrictedNotebookServiceRole

説明: セッションを除くすべての AWS Glue リソースへのフルアクセスを提供します。ユーザーが、ユーザーに関連付けられているノートブックセッションのみを作成して使用できるようにします。このポリシーには、他の AWS サービスの Glue リソースを管理するために Glue が必要とする他のアクセス許可も含まれています AWS 。

AwsGlueSessionUserRestrictedNotebookServiceRole は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AwsGlueSessionUserRestrictedNotebookServiceRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 4 月 18 日 15:27 UTC
- 編集日時: 2024 年 8 月 15 日 20:51 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AwsGlueSessionUserRestrictedNotebookServiceRole

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:tableVersion/*",
        "arn:aws:glue:*:*:connection/*",
        "arn:aws:glue:*:*:userDefinedFunction/*",
        "arn:aws:glue:*:*:devEndpoint/*",
        "arn:aws:glue:*:*:job/*",
        "arn:aws:glue:*:*:trigger/*",
        "arn:aws:glue:*:*:crawler/*",
        "arn:aws:glue:*:*:workflow/*",
        "arn:aws:glue:*:*:mlTransform/*",
        "arn:aws:glue:*:*:registry/*",
        "arn:aws:glue:*:*:schema/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/owner" : "${aws:PrincipalTag/owner}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
    {
      "Sid" : "AllowGlueTaggingAction",
      "Effect" : "Allow",
      "Action" : [
        "glue:TagResource"
      ],
      "Resource" : "arn:aws:glue:*:*:session/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceTag/owner" : "${aws:PrincipalTag/owner}",
          "aws:RequestTag/owner" : "${aws:PrincipalTag/owner}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:RunStatement",
        "glue:GetStatement",
        "glue:ListStatements",
        "glue:CancelStatement",
        "glue:StopSession",
        "glue:DeleteSession",
        "glue:GetSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/owner" : "${aws:PrincipalTag/owner}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:ListSessions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "glue:UntagResource",
        "tag:TagResources",
        "tag:UntagResources"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
```

```
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*/*",
        "arn:aws:s3:::*/*aws-glue-*/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::crawler-public*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
```

```
      ],
      "Resource" : [
        "arn:aws:logs:*:*:/aws-glue/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws-glue-service-resource"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AwsGlueSessionUserRestrictedPolicy

説明: ユーザーに関連付けられたインタラクティブセッションのみ、作成と使用を許可するアクセス許可を提供します。このポリシーには、ユーザーが制限付き Glue セッションロールを渡すことを明示的に許可するアクセス許可も含まれます。

AwsGlueSessionUserRestrictedPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AwsGlueSessionUserRestrictedPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 4 月 14 日 21:31 UTC
- 編集日時: 2024 年 8 月 5 日 23:06 UTC
- ARN: arn:aws:iam::aws:policy/AwsGlueSessionUserRestrictedPolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSessionActions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/owner" : "${aws:userid}"
        },
```

```
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
    {
      "Sid" : "AllowGlueTaggingAction",
      "Effect" : "Allow",
      "Action" : [
        "glue:TagResource"
      ],
      "Resource" : "arn:aws:glue:*:*:session/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/owner" : "${aws:userid}",
          "aws:RequestTag/owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "AllowCompletionActions",
      "Effect" : "Allow",
      "Action" : [
        "glue:StartCompletion",
        "glue:GetCompletion"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:completion/*"
      ]
    },
    {
      "Sid" : "AllowGlueActions",
      "Effect" : "Allow",
      "Action" : [
        "glue:RunStatement",
        "glue:GetStatement",
        "glue:ListStatements",
        "glue:CancelStatement",
        "glue:StopSession",
        "glue:DeleteSession",
        "glue:GetSession"
      ],
```

```
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "AllowListSessions",
      "Effect" : "Allow",
      "Action" : [
        "glue:ListSessions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DenyTagActions",
      "Effect" : "Deny",
      "Action" : [
        "glue:UntagResource",
        "tag:TagResources",
        "tag:UntagResources"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
    {
      "Sid" : "AllowPassRoleActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
```

```
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AwsGlueSessionServiceRoleUserRestricted*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AwsGlueSessionUserRestrictedServiceRole

説明: セッションを除くすべての AWS Glue リソースへのフルアクセスを提供します。ユーザーは、そのユーザーに関連付けられている対話型セッションのみを作成して使用できるようにします。このポリシーには、他の AWS サービスの Glue リソースを管理するために Glue が必要とする他のアクセス許可も含まれています。 AWS

AwsGlueSessionUserRestrictedServiceRole は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AwsGlueSessionUserRestrictedServiceRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 4 月 14 日 21:30 UTC

- 編集日時: 2024 年 8 月 5 日 23:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AwsGlueSessionUserRestrictedServiceRole`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowGlueActions",
      "Effect" : "Allow",
      "Action" : "glue:*",
      "Resource" : [
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:tableVersion/*",
        "arn:aws:glue:*:*:connection/*",
        "arn:aws:glue:*:*:userDefinedFunction/*",
        "arn:aws:glue:*:*:devEndpoint/*",
        "arn:aws:glue:*:*:job/*",
        "arn:aws:glue:*:*:trigger/*",
        "arn:aws:glue:*:*:crawler/*",
        "arn:aws:glue:*:*:workflow/*",
        "arn:aws:glue:*:*:mlTransform/*",
        "arn:aws:glue:*:*:registry/*",
        "arn:aws:glue:*:*:schema/*"
      ]
    },
    {
      "Sid" : "AllowCompletionActions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "glue:StartCompletion",
        "glue:GetCompletion"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:completion/*"
      ]
    },
    {
      "Sid" : "AllowSessionActions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/owner" : "${aws:userid}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
    {
      "Sid" : "AllowGlueTaggingAction",
      "Effect" : "Allow",
      "Action" : [
        "glue:TagResource"
      ],
      "Resource" : "arn:aws:glue:*:*:session/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/owner" : "${aws:userid}",
          "aws:RequestTag/owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "AllowStatementActions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "glue:RunStatement",
        "glue:GetStatement",
        "glue:ListStatements",
        "glue:CancelStatement",
        "glue:StopSession",
        "glue:DeleteSession",
        "glue:GetSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "AllowListSessionsAction",
      "Effect" : "Allow",
      "Action" : [
        "glue:ListSessions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DenyTagActions",
      "Effect" : "Deny",
      "Action" : [
        "glue:UntagResource",
        "tag:TagResources",
        "tag:UntagResources"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "AllowS3BucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*"
      ]
    },
    {
      "Sid" : "AllowS3ObjectActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*/*",
        "arn:aws:s3:::*/*aws-glue-*/*"
      ]
    },
    {
      "Sid" : "AllowS3ObjectCrawlerActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::crawler-public*"
      ]
    },
    {
      "Sid" : "AllowLogsActions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
```

```
      ],
      "Resource" : [
        "arn:aws:logs:*:*:/aws-glue/*"
      ]
    },
    {
      "Sid" : "AllowTagsActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws-glue-service-resource"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSGrafanaAccountAdministrator

説明: 組織全体のワークスペースを作成および管理するための Amazon Grafana 内のアクセスを提供します。

AWSGrafanaAccountAdministrator は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSGrafanaAccountAdministrator をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 2 月 23 日 00:20 UTC
- 編集日時: 2022 年 2 月 15 日 22:36 UTC
- ARN: arn:aws:iam::aws:policy/AWSGrafanaAccountAdministrator

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSGrafanaConsoleReadOnlyAccess

説明: Amazon Grafana の読み取り専用オペレーションへのアクセス。

`AWSGrafanaConsoleReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSGrafanaConsoleReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 2 月 23 日 00:10 UTC
- 編集日時: 2022 年 2 月 15 日 22:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGrafanaConsoleReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSGrafanaWorkspacePermissionManagement

説明: AWS Grafana ワークスペースのユーザーおよびグループのアクセス許可を更新する機能のみを提供します。

AWSGrafanaWorkspacePermissionManagement は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSGrafanaWorkspacePermissionManagement をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 2 月 23 日 00:15 UTC
- 編集日時: 2023 年 3 月 15 日 22:17 UTC
- ARN: arn:aws:iam::aws:policy/AWSGrafanaWorkspacePermissionManagement

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSGrafanaWorkspacePermissionManagementV2

説明: Amazon Managed Grafana ワークスペースの IAM Identity Center (IdC) ユーザーおよびグループのアクセス許可を更新する機能を提供します。

AWSGrafanaWorkspacePermissionManagementV2 は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSGrafanaWorkspacePermissionManagementV2 をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 1 月 5 日 18:39 UTC
- 編集日時: 2024 年 1 月 5 日 18:39 UTC
- ARN: arn:aws:iam::aws:policy/AWSGrafanaWorkspacePermissionManagementV2

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSGreengrassFullAccess

説明: このポリシーは、 AWS Greengrass の設定、管理、デプロイアクションへのフルアクセスを許可します。

`AWSGreengrassFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSGreengrassFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 5 月 3 日 00:47 UTC
- 編集日時: 2017 年 5 月 3 日 00:47 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSGreengrassReadOnlyAccess

説明: このポリシーは、 AWS Greengrass の設定、管理、デプロイアクションへの読み取り専用アクセスを許可します。

`AWSGreengrassReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSGreengrassReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 10 月 30 日 16:01 UTC
- 編集日時: 2018 年 10 月 30 日 16:01 UTC
- ARN: arn:aws:iam::aws:policy/AWSGreengrassReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSGreengrassResourceAccessRolePolicy

説明: Lambda や AWS IoT AWS モノのシャドウなどの関連サービスへのアクセスを許可する AWS Greengrass サービスロールのポリシー。

`AWSGreengrassResourceAccessRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSGreengrassResourceAccessRolePolicy` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2017 年 2 月 14 日 21:17 UTC
- 編集日時: 2018 年 11 月 14 日 00:35 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSGreengrassResourceAccessRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSGroundStationAgentInstancePolicy

説明: AWS Ground Station エージェントを使用するための Dataflow エンドポイントインスタンスのアクセス許可を提供します

`AWSGroundStationAgentInstancePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSGroundStationAgentInstancePolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 3 月 29 日 15:23 UTC
- 編集日時: 2025 年 11 月 20 日 16:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGroundStationAgentInstancePolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "groundstation:RegisterAgent",
        "groundstation:UpdateAgentStatus",
        "groundstation:GetAgentConfiguration",
        "groundstation:GetAgentTaskResponseUrl"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSHealth_EventProcessorServiceRolePolicy

説明: AWS Health が Health イベントプロセッサ機能を有効にできるようにします。

`AWSHealth_EventProcessorServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 1 月 13 日 19:24 UTC
- 編集日時: 2023 年 1 月 13 日 19:24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSHealth_EventProcessorServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSHealthFullAccess

説明: AWS Health Apis and Notifications と Personal Health Dashboard へのフルアクセスを許可します

AWSHealthFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSHealthFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2016 年 12 月 6 日 12:30 UTC
- 編集日時: 2020 年 11 月 16 日 18:11 UTC
- ARN: arn:aws:iam::aws:policy/AWSHealthFullAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSHealthImagingFullAccess

説明: AWS Health Imaging サービスへのフルアクセスを提供します。

`AWSHealthImagingFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSHealthImagingFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 7 月 25 日 23:39 UTC
- 編集日時: 2023 年 7 月 25 日 23:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSHealthImagingFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSHealthImagingReadOnlyAccess

説明: AWS Health Imaging サービスへの読み取り専用アクセスを提供します。

`AWSHealthImagingReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSHealthImagingReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 7 月 25 日 23:40 UTC

- 編集日時: 2023 年 8 月 1 日 15:18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSHealthImagingReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSIAMIdentityCenterAllowListForIdentityContext

説明: IAM Identity Center アイデンティティコンテキストで引き受けられたロールに許可されるアクションのリストを提供します。 AWS Security Token Service (AWS STS) は、引き受けられたロールにこのポリシーを自動的にアタッチします。ID コンテキストは ProvidedContext として渡されます。

`AWSIAMIdentityCenterAllowListForIdentityContext` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSIAMIdentityCenterAllowListForIdentityContext` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 11 月 8 日 15:21 UTC
- 編集日時: 2024 年 10 月 01 日 14:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIAMIdentityCenterAllowListForIdentityContext`

ポリシーのバージョン

ポリシーのバージョン: v12 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
      "Sid" : "TrustedIdentityPropagation",
      "Effect" : "Deny",
      "NotAction" : [
        "aoss:APIAccessAll",
        "athena:BatchGetNamedQuery",
        "athena:BatchGetPreparedStatement",
        "athena:BatchGetQueryExecution",
        "athena:CreateNamedQuery",
        "athena:CreatePreparedStatement",
        "athena:DeleteNamedQuery",
        "athena:DeletePreparedStatement",
        "athena:GetNamedQuery",
        "athena:GetPreparedStatement",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryResultsStream",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetWorkGroup",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements",
        "athena:ListQueryExecutions",
        "athena:StartQueryExecution",
        "athena:StopQueryExecution",
        "athena:UpdateNamedQuery",
        "athena:UpdatePreparedStatement",
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetTableMetadata",
        "athena:ListDatabases",
        "athena:ListDataCatalogs",
        "athena:ListTableMetadata",
        "athena:ListWorkGroups",
        "elasticmapreduce:GetClusterSessionCredentials",
        "elasticmapreduce:AddJobFlowSteps",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:CancelSteps",
        "elasticmapreduce:DescribeStep",
        "elasticmapreduce:ListSteps",
        "es:ESHttpHead",
        "es:ESHttpPost",
        "es:ESHttpGet",
        "es:ESHttpPatch",
        "es:ESHttpDelete",
        "es:ESHttpPut",
```

```
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetTableVersions",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:BatchGetPartition",
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:SearchTables",
        "glue:CreateDatabase",
        "glue:UpdateDatabase",
        "glue:DeleteDatabase",
        "glue:CreateTable",
        "glue:DeleteTable",
        "glue:BatchDeleteTable",
        "glue:UpdateTable",
        "glue:BatchCreatePartition",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
        "glue:UpdatePartition",
        "glue:BatchUpdatePartition",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "lakeformation:GetDataAccess",
        "s3:GetAccessGrantsInstanceForPrefix",
        "s3:GetDataAccess",
        "s3:ListCallerAccessGrants",
        "q:StartConversation",
        "q:SendMessage",
        "q:ListConversations",
        "q:GetConversation",
        "q:StartTroubleshootingAnalysis",
        "q:GetTroubleshootingResults",
        "q:StartTroubleshootingResolutionExplanation",
        "q:UpdateTroubleshootingCommandResult",
        "qapps:CreateQApp",
        "qapps:PredictProblemStatementFromConversation",
        "qapps:PredictQAppFromProblemStatement",
        "qapps:CopyQApp",
```

```
        "qapps:GetQApp",
        "qapps:ListQApps",
        "qapps:UpdateQApp",
        "qapps:DeleteQApp",
        "qapps:AssociateQAppWithUser",
        "qapps:DisassociateQAppFromUser",
        "qapps:ImportDocumentToQApp",
        "qapps:ImportDocumentToQAppSession",
        "qapps:CreateLibraryItem",
        "qapps:GetLibraryItem",
        "qapps:UpdateLibraryItem",
        "qapps:CreateLibraryItemReview",
        "qapps:ListLibraryItems",
        "qapps:CreateSubscriptionToken",
        "qapps:StartQAppSession",
        "qapps:StopQAppSession",
        "qapps:PredictQApp",
        "qapps:ImportDocument",
        "qapps:AssociateLibraryItemReview",
        "qapps:DisassociateLibraryItemReview",
        "qapps:GetQAppSession",
        "qapps:UpdateQAppSession",
        "qapps:GetQAppSessionMetadata",
        "qapps:UpdateQAppSessionMetadata",
        "qapps:TagResource",
        "qapps:ListQAppSessionData",
        "qapps:ExportQAppSessionData",
        "qbusiness:Chat",
        "qbusiness:ChatSync",
        "qbusiness:ListConversations",
        "qbusiness:ListMessages",
        "qbusiness:DeleteConversation",
        "qbusiness:PutFeedback",
        "sts:SetContext"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する

- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSIdentityCenterExternalManagementPolicy

説明: 外部プロバイダーから IAM Identity Center ユーザーを管理するためのアクセスを提供します。

AWSIdentityCenterExternalManagementPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIdentityCenterExternalManagementPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2025 年 11 月 22 日 00:34 UTC
- 編集日時: 2025 年 12 月 5 日 20:34 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIdentityCenterExternalManagementPolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
      "Effect" : "Allow",
      "Action" : [
        "identitystore:CreateUser"
      ],
      "Resource" : [
        "arn:aws:identitystore::*:identitystore/${aws:PrincipalTag/IdentityStoreId}",
        "arn:aws:identitystore:::user/*"
      ],
      "Condition" : {
        "ForAllValues:ArnEquals" : {
          "identitystore:UserExternalIdIssuers" : [
            "arn:aws:identitystore::*:identitystore/${aws:PrincipalTag/
IdentityStoreId}/provisioningtenant/${aws:PrincipalTag/IdentityStoreExternalIdIssuer}"
          ]
        },
        "Null" : {
          "identitystore:UserExternalIdIssuers" : "false",
          "identitystore:ReservedUserId" : "false"
        }
      }
    },
    {
      "Sid" : "IdentityStoreUserManagement",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:UpdateUser",
        "identitystore:DeleteUser",
        "identitystore:DescribeUser"
      ],
      "Resource" : [
        "arn:aws:identitystore::*:identitystore/${aws:PrincipalTag/IdentityStoreId}",
        "arn:aws:identitystore:::user/*"
      ],
      "Condition" : {
        "ForAllValues:ArnEquals" : {
          "identitystore:UserExternalIdIssuers" : [
            "arn:aws:identitystore::*:identitystore/${aws:PrincipalTag/
IdentityStoreId}/provisioningtenant/${aws:PrincipalTag/IdentityStoreExternalIdIssuer}"
          ]
        },
        "Null" : {
          "identitystore:UserExternalIdIssuers" : "false"
        }
      }
```

```
    },
    {
      "Sid" : "IdentityStoreCMKAccess",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" : [
            "arn:aws:identitystore::${aws:PrincipalAccount}:identitystore/
${aws:PrincipalTag/IdentityStoreId}"
          ]
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSIdentitySyncFullAccess

説明: Identity Sync サービスへのフルアクセスを付与

`AWSIdentitySyncFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSIdentitySyncFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 3 月 23 日 23:29 UTC
- 編集日時: 2022 年 3 月 23 日 23:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIdentitySyncFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSIdentitySyncReadOnlyAccess

説明: Identity Sync サービスへの読み取り専用アクセス

`AWSIdentitySyncReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSIdentitySyncReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 3 月 23 日 23:29 UTC
- 編集日時: 2022 年 3 月 23 日 23:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIdentitySyncReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "identity-sync:GetSyncProfile",
        "identity-sync:ListSyncFilters",
        "identity-sync:GetSyncTarget"
      ],
      "Resource" : "arn:*:identity-sync:*:*:*/*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSImageBuilderFullAccess

説明: すべての AWS Image Builder アクションへのフルアクセスと、関連 AWS サービスへのリソーススコープアクセスを提供します。

`AWSImageBuilderFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSImageBuilderFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 12 月 20 日 18:25 UTC
- 編集日時: 2021 年 4 月 13 日 17:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSImageBuilderFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSImageBuilderReadOnlyAccess

説明: すべての AWS Image Builder アクションへの読み取り専用アクセスを提供します。

`AWSImageBuilderReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSImageBuilderReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 12 月 19 日 22:29 UTC
- 編集日時: 2019 年 12 月 19 日 22:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSImageBuilderReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
```

```
  "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"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSImportExportFullAccess

説明: AWS アカウントで作成されたジョブへの読み取りおよび書き込みアクセスを提供します。

`AWSImportExportFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSImportExportFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2015 年 2 月 6 日 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSImportExportFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSImportExportReadOnlyAccess

説明: AWS アカウントで作成されたジョブに対する読み取り専用アクセス権を付与します。

AWSImportExportReadOnlyAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSImportExportReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2015 年 2 月 6 日 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AWSImportExportReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSIncidentManagerIncidentAccessServiceRolePolicy

説明: インシデントの管理の一環として他の AWS サービスを呼び出すアクセス許可を Incident Manager に付与します。

`AWSIncidentManagerIncidentAccessServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSIncidentManagerIncidentAccessServiceRolePolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 11 月 13 日 00:01 UTC
- 編集日時: 2024 年 2 月 20 日 23:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIncidentManagerIncidentAccessServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IncidentAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources",
        "codedeploy:BatchGetDeployments",
        "codedeploy:ListDeployments",
        "codedeploy:ListDeploymentTargets",
        "autoscaling:DescribeAutoScalingInstances"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSIncidentManagerResolverAccess

説明: このポリシーでは、インシデントを開始、表示、更新するアクセス許可と、カスタムタイムラインイベントおよび関連項目へのフルアクセス権を付与します。インシデントを作成および解決するユーザーにこのポリシー割り当ててください。

AWSIncidentManagerResolverAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIncidentManagerResolverAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 5 月 10 日 06:12 UTC
- 編集日時: 2025 年 11 月 20 日 18:49 UTC
- ARN: arn:aws:iam::aws:policy/AWSIncidentManagerResolverAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "StartIncidentPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-incidents:StartIncident",
        "ssm-contacts:StartEngagement"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ResponsePlanReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-incidents:ListResponsePlans",
```

```
        "ssm-incidents:GetResponsePlan"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IncidentRecordResolverPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-incidents:ListIncidentRecords",
        "ssm-incidents:GetIncidentRecord",
        "ssm-incidents:UpdateIncidentRecord",
        "ssm-incidents:ListTimelineEvents",
        "ssm-incidents:CreateTimelineEvent",
        "ssm-incidents:GetTimelineEvent",
        "ssm-incidents:UpdateTimelineEvent",
        "ssm-incidents:DeleteTimelineEvent",
        "ssm-incidents:ListRelatedItems",
        "ssm-incidents:UpdateRelatedItems"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSIncidentManagerServiceRolePolicy

説明: このポリシーは、Indent Manager が ユーザーに代わって Incident レコードと関連リソースを管理するためのアクセス許可を付与します。

`AWSIncidentManagerServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 5 月 10 日 03:34 UTC
- 編集日時: 2025 年 1 月 28 日 02:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIncidentManagerServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "UpdateIncidentRecordPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-incidents:ListIncidentRecords",
        "ssm-incidents:CreateTimelineEvent"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RelatedOpsItemPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ssm:CreateOpsItem",
        "ssm:AssociateOpsItemRelatedItem"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IncidentEngagementPermissions",
      "Effect" : "Allow",
      "Action" : "ssm-contacts:StartEngagement",
      "Resource" : "*"
    },
    {
      "Sid" : "PutMetricDataPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/IncidentManager",
            "AWS/Usage"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSIoT1ClickFullAccess

説明: AWS IoT 1-Click へのフルアクセスを提供します。

AWSIoT1ClickFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIoT1ClickFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 5 月 11 日 22:10 UTC
- 編集日時: 2018 年 5 月 11 日 22:10 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoT1ClickFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "iot1click:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSIoT1ClickReadOnlyAccess

説明: AWS IoT 1-Click への読み取り専用アクセスを提供します。

AWSIoT1ClickReadOnlyAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIoT1ClickReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 5 月 11 日 21:49 UTC
- 編集日時: 2018 年 5 月 11 日 21:49 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoT1ClickReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "iot1click:Describe*",
        "iot1click:Get*",
        "iot1click:List*"
      ],
```

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSIoTAnalyticsFullAccess

説明: IoT 分析 へのフルアクセスを提供します。

`AWSIoTAnalyticsFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSIoTAnalyticsFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 6 月 18 日 23:02 UTC
- 編集日時: 2018 年 6 月 18 日 23:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTAnalyticsFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSIoTAnalyticsReadOnlyAccess

説明: IoT 分析 への読み取り専用アクセスを提供します。

`AWSIoTAnalyticsReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSIoTAnalyticsReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 6 月 18 日 21:37 UTC
- 編集日時: 2018 年 6 月 18 日 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTAnalyticsReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSIoTConfigAccess

説明: このポリシーは、 AWS IoT 設定アクションへのフルアクセスを許可します

AWSIoTConfigAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIoTConfigAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 10 月 27 日 21:52 UTC
- 編集日時: 2019 年 9 月 27 日 20:48 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTConfigAccess

ポリシーのバージョン

ポリシーのバージョン: v9 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSIoTConfigReadOnlyAccess

説明: このポリシーは、 AWS IoT 設定アクションへの読み取り専用アクセスを許可します

`AWSIoTConfigReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSIoTConfigReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 10 月 27 日 21:52 UTC
- 編集日時: 2019 年 9 月 27 日 20:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTConfigReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSIoTDataAccess

説明: このポリシーは、 AWS IoT メッセージングアクションへのフルアクセスを許可します

`AWSIoTDataAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSIoTDataAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 10 月 27 日 21:51 UTC
- 編集日時: 2021 年 6 月 23 日 21:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTDataAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction

説明: ADD_THINGS_TO_THING_GROUP 緩和アクションを実行するための IoT Thing グループへの書き込みアクセスと IoT 証明書への読み取りアクセスを提供します

`AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2019 年 8 月 7 日 17:55 UTC
- 編集日時: 2019 年 8 月 7 日 17:55 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSIoTDeviceDefenderAudit

説明: IoT および関連リソースの読み取りアクセスを提供します

AWSIoTDeviceDefenderAudit は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIoTDeviceDefenderAudit をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2018 年 7 月 18 日 21:17 UTC
- 編集日時: 2019 年 11 月 25 日 23:52 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderAudit

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
```

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction

説明: ENABLE_IOT_LOGGING 緩和アクションを実行するための IoT ロギングを有効にするためのアクセスを提供します

AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2019 年 8 月 7 日 17:04 UTC
- 編集日時: 2019 年 8 月 7 日 17:04 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
        "iot:SetV2LoggingOptions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "iot.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction

説明: PUBLISH_FINDING_TO_SNS 緩和アクションを実行するための SNS トピックへのメッセージ公開アクセスを提供します

AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2019 年 8 月 7 日 17:04 UTC
- 編集日時: 2019 年 8 月 7 日 17:04 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction

説明: REPLACE_DEFAULT_POLICY_VERSION 緩和アクションを実行するための IoT ポリシーへの書き込みアクセスを提供します

`AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2019 年 8 月 7 日 17:04 UTC
- 編集日時: 2019 年 8 月 7 日 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSIoTDeviceDefenderUpdateCACertMitigationAction

説明: UPDATE_CA_CERTIFICATE 緩和アクションを実行するための IoT CA 証明書への書き込みアクセスを提供します

`AWSIoTDeviceDefenderUpdateCACertMitigationAction` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSIoTDeviceDefenderUpdateCACertMitigationAction` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー

- 作成日時: 2019 年 8 月 7 日 17:05 UTC
- 編集日時: 2019 年 8 月 7 日 17:05 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderUpdateCACertMitigationAction`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction

説明: UPDATE_DEVICE_CERTIFICATE 緩和アクションを実行するための IoT 証明書への書き込みアクセスを提供します

AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2019 年 8 月 7 日 17:06 UTC
- 編集日時: 2019 年 8 月 7 日 17:06 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSIoTDeviceTesterForFreeRTOSFullAccess

説明: IoT、S3、IAM などのサービスへのアクセスを許可することで、 AWS IoT Device Tester が FreeRTOS 認定スイートを実行できるようにします

`AWSIoTDeviceTesterForFreeRTOSFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSIoTDeviceTesterForFreeRTOSFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 2 月 12 日 20:33 UTC
- 編集日時: 2023 年 8 月 10 日 20:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTDeviceTesterForFreeRTOSFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSIoTDeviceTesterForGreengrassFullAccess

説明: Lambda、IoT、API Gateway、IAM などの関連サービスへのアクセスを許可することで、AWS IoT Device Tester が AWS Greengrass 認定スイートを実行できるようにします

`AWSIoTDeviceTesterForGreengrassFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSIoTDeviceTesterForGreengrassFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 2 月 20 日 21:21 UTC
- 編集日時: 2020 年 6 月 25 日 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTDeviceTesterForGreengrassFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSIoTEventsFullAccess

説明: IoT イベントへのフルアクセスを提供します。

AWSIoTEventsFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIoTEventsFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 1 月 10 日 22:51 UTC
- 編集日時: 2019 年 1 月 10 日 22:51 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTEventsFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
    {
      "Effect" : "Allow",
      "Action" : [
        "iotevents:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSIoTEventsReadOnlyAccess

説明: IoT イベントへの読み取り専用アクセスを提供します。

`AWSIoTEventsReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSIoTEventsReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 1 月 10 日 22:50 UTC
- 編集日時: 2019 年 9 月 23 日 17:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTEventsReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSIoTFleetHubFederationAccess

説明: IoT フリート Hub アプリケーションへのフェデレーションアクセス

`AWSIoTFleetHubFederationAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSIoTFleetHubFederationAccess` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 12 月 15 日 08:08 UTC
- 編集日時: 2022 年 4 月 4 日 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTFleetHubFederationAccess`

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSIoTFleetwiseServiceRolePolicy

説明: AWSIoTFleetwise が補助機能に使用または管理する AWS リソースとmetaDataにアクセス許可を付与します

`AWSIoTFleetwiseServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 9 月 21 日 23:27 UTC
- 編集日時: 2025 年 10 月 16 日 04:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTFleetwiseServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSIoTFullAccess

説明: このポリシーは、 AWS IoT 設定およびメッセージングアクションへのフルアクセスを許可します。

AWSIoTFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIoTFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 10 月 8 日 15:19 UTC
- 編集日時: 2022 年 5 月 19 日 21:39 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSIoTLogging

説明: Amazon CloudWatch Log グループを作成し、そのグループにログをストリーミングすることを許可します

AWSIoTLogging は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIoTLogging をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 10 月 8 日 15:17 UTC
- 編集日時: 2015 年 10 月 8 日 15:17 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTLogging

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:PutMetricFilter",
        "logs:PutRetentionPolicy",
        "logs:GetLogEvents",
        "logs:DeleteLogStream"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSIoTManagedIntegrationsFullAccess

説明: AWS IoT Device Management および関連サービスのマネージド統合へのフルアクセスを提供します。

`AWSIoTManagedIntegrationsFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSIoTManagedIntegrationsFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 3 月 5 日 19:22 UTC
- 編集日時: 2025 年 3 月 5 日 19:22 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSIoTManagedIntegrationsRolePolicy

説明: AWS IoT Device Management のマネージド統合に、ユーザーに代わってログとメトリクスを発行するアクセス許可を提供します。

AWSIoTManagedIntegrationsRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2025 年 3 月 5 日 21:22 UTC
- 編集日時: 2025 年 3 月 5 日 21:22 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSIoTManagedIntegrationsRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/iotmanagedintegrations/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    },
    {
      "Sid" : "CloudWatchStreams",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/iotmanagedintegrations/*:log-stream:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    },
    {
      "Sid" : "CloudWatchMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/IoTManagedIntegrations",
            "AWS/Usage"
          ]
        }
      }
    }
  ]
```

```
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSIoTOTAUpdate

説明: create AWS IoT ジョブへのアクセスを許可し、 AWS コード署名者ジョブを記述する

AWSIoTOTAUpdate は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIoTOTAUpdate をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2017 年 12 月 20 日 20:36 UTC
- 編集日時: 2017 年 12 月 20 日 20:36 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTOTAUpdate

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
    "Effect" : "Allow",
    "Action" : [
      "iot:CreateJob",
      "signer:DescribeSigningJob"
    ],
    "Resource" : "*"
  }
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSIotRoboRunnerFullAccess

説明: このポリシーは、 AWS Iot RoboRunner へのフルアクセスを許可するアクセス許可を付与します。

`AWSIotRoboRunnerFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSIotRoboRunnerFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 11 月 29 日 03:54 UTC
- 編集日時: 2023 年 2 月 23 日 18:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIotRoboRunnerFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSIotRoboRunnerReadOnly

説明: このポリシーは、 AWS Iot RoboRunner への読み取り専用アクセスを許可するアクセス許可を付与します。

AWSIotRoboRunnerReadOnly は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIotRoboRunnerReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 11 月 29 日 03:43 UTC
- 編集日時: 2022 年 11 月 16 日 20:51 UTC
- ARN: arn:aws:iam::aws:policy/AWSIotRoboRunnerReadOnly

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSIotRoboRunnerServiceRolePolicy

説明: AWS IoT RoboRunner が顧客に代わって関連する AWS リソースを管理できるようにします。

`AWSIotRoboRunnerServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 2 月 21 日 16:56 UTC
- 編集日時: 2023 年 2 月 21 日 16:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIotRoboRunnerServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSIoTRuleActions

説明: AWS IoT ルールアクションでサポートされているすべての AWS サービスへのアクセスを許可します

AWSIoTRuleActions は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIoTRuleActions をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 10 月 8 日 15:14 UTC

- 編集日時: 2018 年 1 月 16 日 19:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTRuleActions`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSIoTSiteWiseConsoleFullAccess

説明: を使用して、 AWS IoT SiteWise を管理するためのフルアクセスを提供します AWS マネジメントコンソール。このポリシーは、 AWS IoT SiteWise で使用されるデータストアの作成と一覧表示 (AWS IoT Analytics など)、 AWS IoT Greengrass リソースの一覧表示と表示、 AWS Secrets Manager シークレットの一覧表示と変更、 AWS IoT モノのシャドウの取得、特定のタグを持つリソースの一覧表示、 AWS IoT SiteWise のサービスにリンクされたロールの作成と使用のためのアクセスも許可することに注意してください。

`AWSIoTSiteWiseConsoleFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSIoTSiteWiseConsoleFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 5 月 31 日 21:37 UTC
- 編集日時: 2019 年 5 月 31 日 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTSiteWiseConsoleFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSIoTSiteWiseFullAccess

説明: IoT SiteWise へのフルアクセスを提供します。

AWSIoTSiteWiseFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIoTSiteWiseFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 12 月 4 日 20:53 UTC
- 編集日時: 2018 年 12 月 4 日 20:53 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTSiteWiseFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSIoTSiteWiseMonitorPortalAccess

説明: このポリシーは、 AWS IoT SiteWise アセットとアセットデータにアクセスし、 AWS IoT SiteWise Monitor リソースを作成し、SSO ユーザーを一覧表示するアクセス許可を付与 AWS します。

`AWSIoTSiteWiseMonitorPortalAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSIoTSiteWiseMonitorPortalAccess` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 5 月 19 日 20:01 UTC
- 編集日時: 2020 年 5 月 19 日 20:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTSiteWiseMonitorPortalAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSIoTSiteWiseMonitorServiceRolePolicy

説明: このロールは、 AWS IoT SiteWise アセットとアセットプロパティにアクセスし、 AWS IoT AWS IoT SiteWise ポータルを通じて IoT Sitewise プロジェクト、ダッシュボード、アクセスポリシーを作成するアクセス許可を、 AWS IoT SiteWise モニターに付与します。

`AWSIoTSiteWiseMonitorServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 11 月 14 日 00:59 UTC
- 編集日時: 2019 年 12 月 13 日 22:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTSiteWiseMonitorServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSIoTSiteWiseReadOnlyAccess

説明: IoT SiteWise への読み取り専用アクセスを提供します。

`AWSIoTSiteWiseReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSIoTSiteWiseReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 12 月 4 日 20:55 UTC
- 編集日時: 2025 年 10 月 29 日 20:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTSiteWiseReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
        "iotsitewise:BatchGetAssetPropertyAggregates",
        "iotsitewise:BatchGetAssetPropertyValue",
        "iotsitewise:BatchGetAssetPropertyValueHistory",
        "iotsitewise:DescribeAccessPolicy",
        "iotsitewise:DescribeAction",
        "iotsitewise:DescribeAsset",
        "iotsitewise:DescribeAssetCompositeModel",
        "iotsitewise:DescribeAssetModel",
        "iotsitewise:DescribeAssetModelCompositeModel",
        "iotsitewise:DescribeAssetModelInterfaceRelationship",
        "iotsitewise:DescribeAssetProperty",
        "iotsitewise:DescribeBulkImportJob",
        "iotsitewise:DescribeComputationModel",
        "iotsitewise:DescribeComputationModelExecutionSummary",
        "iotsitewise:DescribeDashboard",
        "iotsitewise:DescribeDataset",
        "iotsitewise:DescribeDefaultEncryptionConfiguration",
        "iotsitewise:DescribeExecution",
        "iotsitewise:DescribeGateway",
        "iotsitewise:DescribeGatewayCapabilityConfiguration",
        "iotsitewise:DescribeLoggingOptions",
        "iotsitewise:DescribePortal",
        "iotsitewise:DescribeProject",
        "iotsitewise:DescribeStorageConfiguration",
        "iotsitewise:DescribeTimeSeries",
        "iotsitewise:ExecuteQuery",
        "iotsitewise:GetAssetPropertyAggregates",
        "iotsitewise:GetAssetPropertyValue",
        "iotsitewise:GetAssetPropertyValueHistory",
        "iotsitewise:GetInterpolatedAssetPropertyValues",
        "iotsitewise:ListAccessPolicies",
        "iotsitewise:ListActions",
        "iotsitewise:ListAssetModelCompositeModels",
        "iotsitewise:ListAssetModelProperties",
        "iotsitewise:ListAssetModels",
        "iotsitewise:ListAssetProperties",
        "iotsitewise:ListAssetRelationships",
        "iotsitewise:ListAssets",
        "iotsitewise:ListAssociatedAssets",
        "iotsitewise:ListBulkImportJobs",
        "iotsitewise:ListCompositionRelationships",
        "iotsitewise:ListComputationModelDataBindingUsages",
        "iotsitewise:ListComputationModelResolveToResources",
        "iotsitewise:ListComputationModels",
```

```
        "iotsitewise:ListDashboards",
        "iotsitewise:ListDatasets",
        "iotsitewise:ListExecutions",
        "iotsitewise:ListGateways",
        "iotsitewise:ListInterfaceRelationships",
        "iotsitewise:ListPortals",
        "iotsitewise:ListProjectAssets",
        "iotsitewise:ListProjects",
        "iotsitewise:ListTagsForResource",
        "iotsitewise:ListTimeSeries"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSIoTThingsRegistration

説明: このポリシーにより、ユーザーは AWS IoT StartThingRegistrationTask API を使用してモノを一括登録できます。

`AWSIoTThingsRegistration` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSIoTThingsRegistration` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2017 年 12 月 1 日 20:21 UTC

- 編集日時: 2020 年 10 月 5 日 19:20 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTThingsRegistration

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSIoTTwinMakerServiceRolePolicy

説明: AWS IoT TwinMaker が他の AWS サービスを呼び出し、ユーザーに代わってリソースを同期できるようにします。

AWSIoTTwinMakerServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー

- 作成日時: 2023 年 11 月 13 日 18:59 UTC
- 編集日時: 2023 年 11 月 13 日 18:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTTwinMakerServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSIoTWirelessDataAccess

説明: 関連付けられた ID データに AWS IoT Wireless デバイスへのアクセスを許可します。

AWSIoTWirelessDataAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIoTWirelessDataAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 12 月 15 日 15:31 UTC
- 編集日時: 2020 年 12 月 15 日 15:31 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTWirelessDataAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSIoTWirelessFullAccess

説明: 関連付けられた ID にすべての AWS IoT Wireless オペレーションへのフルアクセスを許可します。

`AWSIoTWirelessFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSIoTWirelessFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 12 月 15 日 15:27 UTC
- 編集日時: 2020 年 12 月 15 日 15:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSIoTWirelessFullPublishAccess

説明: IoT Wireless に、お客様のために IoT Rules Engine に対するパブリッシュを実行するためのフルアクセス権限を提供します。

`AWSIoTWirelessFullPublishAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSIoTWirelessFullPublishAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 12 月 15 日 15:29 UTC
- 編集日時: 2020 年 12 月 15 日 15:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessFullPublishAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSIoTWirelessGatewayCertManager

説明: 関連付けられた ID に、IoT 証明書を作成、一覧表示、および記述するためのアクセスを提供します。

AWSIoTWirelessGatewayCertManager は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIoTWirelessGatewayCertManager をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 12 月 15 日 15:30 UTC
- 編集日時: 2020 年 12 月 15 日 15:30 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTWirelessGatewayCertManager

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IoTWirelessGatewayCertManager",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateKeysAndCertificate",
        "iot:DescribeCertificate",
        "iot:ListCertificates"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSIoTWirelessLogging

説明: 関連付けられた ID に、Amazon CloudWatch Logs グループを作成し、グループにログをストリーミングするための許可を付与します。

`AWSIoTWirelessLogging` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSIoTWirelessLogging` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 12 月 15 日 15:32 UTC
- 編集日時: 2020 年 12 月 15 日 15:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessLogging`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
```

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSIoTWirelessReadOnlyAccess

説明: 関連付けられた ID に AWS IoT Wireless への読み取り専用アクセスを許可します。

`AWSIoTWirelessReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSIoTWirelessReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 12 月 15 日 15:28 UTC
- 編集日時: 2020 年 12 月 15 日 15:28 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSIPAMServiceRolePolicy

説明: VPC IP Address Manager が VPC リソースにアクセスし、ユーザーに代わって AWS Organizations と統合できるようにします。

`AWSIPAMServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 11 月 30 日 19:08 UTC
- 編集日時: 2025 年 10 月 28 日 00:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIPAMServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IPAMDiscoveryDescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeByoipCidrs",
        "ec2:DescribeIpv6Pools",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePublicIpv4Pools",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
```

```
        "ec2:DescribeVpnConnections",
        "ec2:GetIpamDiscoveredAccounts",
        "ec2:GetIpamDiscoveredPublicAddresses",
        "ec2:GetIpamDiscoveredResourceCidrs",
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListByoipCidrs",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:DescribeOrganizationalUnit",
        "cloudfront:ListAnycastIpLists",
        "cloudfront:ListDistributionsByAnycastIpListId",
        "cloudfront:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchMetricsPublishActions",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/IPAM"
        }
      }
    },
    {
      "Sid" : "IPAMAllocationPolicyActions",
      "Effect" : "Allow",
      "Action" : "ec2:AllocateIpamPoolCidr",
      "Resource" : "*"
    },
    {
      "Sid" : "PrefixListResolverWriteActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyManagedPrefixList"
      ],
      "Resource" : [
        "*"
```

```
      ],
      "Condition" : {
        "Null" : {
          "ec2:Attribute/ExpectedIpamPrefixListResolverTarget" : "false"
        }
      }
    },
    {
      "Sid" : "PrefixListResolverReadActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeManagedPrefixLists",
        "ec2:GetManagedPrefixListEntries"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSIQContractServiceRolePolicy

説明: IQ AWS が顧客に代わって支払いリクエストを実行するために使用されます

AWSIQContractServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー

- 作成日時: 2019 年 8 月 22 日 19:28 UTC
- 編集日時: 2019 年 8 月 22 日 19:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIQContractServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSIQFullAccess

説明: IQ AWS へのフルアクセスを提供します

`AWSIQFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIQFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 4 月 4 日 23:13 UTC
- 編集日時: 2019 年 9 月 25 日 20:22 UTC
- ARN: arn:aws:iam::aws:policy/AWSIQFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSIQPermissionServiceRolePolicy

説明: IQ AWS エキスパートが引き受けるロールの管理を IQ AWS に許可します。

AWSIQPermissionServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 8 月 22 日 19:36 UTC
- 編集日時: 2019 年 8 月 22 日 19:36 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSIQPermissionServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy

説明: KMS AWS カスタムキーストアに必要な AWS サービスとリソースへのアクセスを有効にします

AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 11 月 14 日 20:10 UTC
- 編集日時: 2023 年 11 月 10 日 19:03 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy

説明: KMS AWS がマルチリージョンキーの共有プロパティを同期できるようにします。

AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 6 月 16 日 15:37 UTC
- 編集日時: 2024 年 11 月 13 日 22:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSKeyManagementServicePowerUser

説明: AWS Key Management Service (KMS) へのアクセスを提供します。

AWSKeyManagementServicePowerUser は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSKeyManagementServicePowerUser をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2017 年 3 月 7 日 00:55 UTC
- ARN: arn:aws:iam::aws:policy/AWSKeyManagementServicePowerUser

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSLakeFormationCrossAccountManager

説明: Lake Formation を経由した Glue リソースへのクロスアカウントアクセスを提供します。組織やリソースアクセスマネージャーなど、他の必要なサービスへの読み取りアクセスも付与します

`AWSLakeFormationCrossAccountManager` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSLakeFormationCrossAccountManager` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 8 月 4 日 20:59 UTC
- 編集日時: 2025 年 2 月 25 日 00:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLakeFormationCrossAccountManager`

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCreateResourceShare",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "ram:RequestedResourceType" : [
            "glue:Table",
            "glue:Database",
            "glue:Catalog"
          ]
        }
      }
    },
    {
      "Sid" : "AllowManageResourceShare",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ram:UpdateResourceShare",
        "ram:DeleteResourceShare",
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare",
        "ram:GetResourceShares"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ram:ResourceShareName" : [
            "LakeFormation*"
          ]
        }
      }
    },
    {
      "Sid" : "AllowManageResourceSharePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:AssociateResourceSharePermission"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ram:PermissionArn" : [
            "arn:aws:ram::aws:permission/AWSRAMLFEnabled*"
          ]
        }
      }
    },
    {
      "Sid" : "AllowXAcctManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:PutResourcePolicy",
        "glue:DeleteResourcePolicy",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "ram:Get*",
        "ram:List*"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "AllowOrganizationsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListRoots",
        "organizations:ListAccountsForParent",
        "organizations:ListOrganizationalUnitsForParent"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSLakeFormationDataAdmin

説明: データレイクを管理するための AWS Lake Formation および AWS Glue などの関連サービスへの管理アクセスを付与します

AWSLakeFormationDataAdmin は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSLakeFormationDataAdmin をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 8 月 8 日 17:33 UTC
- 編集日時: 2024 年 12 月 3 日 15:06 UTC
- ARN: arn:aws:iam::aws:policy/AWSLakeFormationDataAdmin

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSLakeFormationDataAdminAllow",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:*",
        "cloudtrail:DescribeTrails",
        "cloudtrail:LookupEvents",
        "glue:CreateCatalog",
        "glue:UpdateCatalog",
        "glue:DeleteCatalog",
        "glue:GetCatalog",
        "glue:GetCatalogs",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:CreateDatabase",
        "glue:UpdateDatabase",
        "glue:DeleteDatabase",
        "glue:GetConnections",
        "glue:SearchTables",
        "glue:GetTable",
        "glue:CreateTable",
        "glue:UpdateTable",
        "glue:DeleteTable",
        "glue:GetTableVersions",
        "glue:GetPartitions",
        "glue:GetTables",
        "glue:ListWorkflows",
        "glue:BatchGetWorkflows",
        "glue:DeleteWorkflow",
        "glue:GetWorkflowRuns",
```

```
        "glue:StartWorkflowRun",
        "glue:GetWorkflow",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "iam:ListUsers",
        "iam:ListRoles",
        "iam:GetRole",
        "iam:GetRolePolicy"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSLakeFormationDataAdminDeny",
      "Effect" : "Deny",
      "Action" : [
        "lakeformation:PutDataLakeSettings"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSLambda_FullAccess

説明: AWS Lambda サービス、 AWS Lambda コンソール機能、およびその他の関連 AWS サービスへのフルアクセスを許可します。

`AWSLambda_FullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSLambda_FullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 11 月 17 日 21:14 UTC
- 編集日時: 2025 年 12 月 1 日 16:04 UTC
- ARN: arn:aws:iam::aws:policy/AWSLambda_FullAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricData",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "kms:DescribeKey",
        "kms:ListAliases",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",
```

```
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "lambda:*",
        "logs:DescribeLogGroups",
        "states:DescribeStateMachine",
        "states:ListStateMachines",
        "tag:GetResources",
        "xray:GetTraceSummaries",
        "xray:BatchGetTraces"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "logs:FilterLogEvents",
        "logs:StartLiveTail",
        "logs:StopLiveTail"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/lambda/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/lambda.amazonaws.com/
AWSServiceRoleForLambda",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "lambda.amazonaws.com"
        }
      }
```

```
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSLambda_ReadOnlyAccess

説明: AWS Lambda サービス、 AWS Lambda コンソール機能、およびその他の関連 AWS サービスへの読み取り専用アクセスを許可します。

`AWSLambda_ReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSLambda_ReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 11 月 17 日 21:10 UTC
- 編集日時: 2025 年 3 月 17 日 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambda_ReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks",
        "cloudformation:ListStackResources",
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "kms:ListAliases",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "logs:DescribeLogGroups",
        "lambda:Get*",
        "lambda:List*",
        "states:DescribeStateMachine",
        "states:ListStateMachines",
        "tag:GetResources",
        "xray:GetTraceSummaries",
        "xray:BatchGetTraces"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "logs:FilterLogEvents",
        "logs:StartQuery",
        "logs:StopQuery",
```

```
        "logs:DescribeQueries",
        "logs:GetLogGroupFields",
        "logs:GetLogRecord",
        "logs:GetQueryResults",
        "logs:StartLiveTail",
        "logs:StopLiveTail"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/lambda/*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSLambdaBasicDurableExecutionRolePolicy

説明: CloudWatch Logs への書き込みアクセス許可と、Lambda の耐久性のある関数で使用される耐久性のある実行 APIs への読み取り/書き込みアクセス許可を提供します

AWSLambdaBasicDurableExecutionRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSLambdaBasicDurableExecutionRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2025 年 12 月 2 日 15:04 UTC
- 編集日時: 2025 年 12 月 2 日 15:04 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSLambdaBasicDurableExecutionRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "lambda:CheckpointDurableExecution",
        "lambda:GetDurableExecutionState"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSLambdaBasicExecutionRole

説明: CloudWatch Logs への書き込み権限を提供します。

AWSLambdaBasicExecutionRole は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSLambdaBasicExecutionRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 4 月 9 日 15:03 UTC
- 編集日時: 2015 年 4 月 9 日 15:03 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する

- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSLambdaDynamoDBExecutionRole

説明: DynamoDB ストリームへのリストアップおよび読み取りアクセス、および CloudWatch ログへの書き込みアクセスを提供します。

AWSLambdaDynamoDBExecutionRole は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSLambdaDynamoDBExecutionRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 4 月 9 日 15:09 UTC
- 編集日時: 2015 年 4 月 9 日 15:09 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSLambdaDynamoDBExecutionRole

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
      "Action" : [
        "dynamodb:DescribeStream",
        "dynamodb:GetRecords",
        "dynamodb:GetShardIterator",
        "dynamodb:ListStreams",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSLambdaENIManagementAccess

説明: Lambda 関数に、VPC 対応 Lambda 関数が使用する ENI (作成、記述、削除) を管理するための最低限の権限を提供します。

`AWSLambdaENIManagementAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSLambdaENIManagementAccess` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2016 年 12 月 6 日 00:37 UTC
- 編集日時: 2020 年 10 月 1 日 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaENIManagementAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSLambdaExecute

説明: PUT リクエスト、S3 に対するアクセス取得、および CloudWatch ログへのフルアクセスを提供します。

AWSLambdaExecute は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSLambdaExecute をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2015 年 2 月 6 日 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AWSLambdaExecute

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:*"
      ],
      "Resource" : "arn:aws:logs:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
      ],
```

```
      "Resource" : "arn:aws:s3:::*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSLambdaFullAccess

説明: このポリシーは非推奨化される予定です。ガイダンスについては、「https://docs.aws.amazon.com/lambda/latest/dg/access-control-identity-based.html」のドキュメントを参照してください。Lambda、S3、DynamoDB、CloudWatch メトリクス、ログへのフルアクセスを提供します。

`AWSLambdaFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSLambdaFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2017 年 11 月 27 日 23:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambdaFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSLambdaInvocation-DynamoDB

説明: DynamoDB ストリームへの読み取りアクセスを提供します。

AWSLambdaInvocation-DynamoDB は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSLambdaInvocation-DynamoDB をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2015 年 2 月 6 日 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AWSLambdaInvocation-DynamoDB

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeStream",
        "dynamodb:GetRecords",
        "dynamodb:GetShardIterator",
        "dynamodb:ListStreams"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSLambdaKinesisExecutionRole

説明: Kinesis ストリームへのリストアップおよび読み取りアクセス、および CloudWatch ログへの書き込みアクセスを提供します。

`AWSLambdaKinesisExecutionRole` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSLambdaKinesisExecutionRole` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 4 月 9 日 15:14 UTC
- 編集日時: 2018 年 11 月 19 日 20:09 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaKinesisExecutionRole`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSLambdaManagedEC2ResourceOperator

説明: このポリシーは、Lambda マネージドインスタンスによって管理される EC2 リソースを作成および管理するためのアクセス許可と、説明的なアクセス許可を に付与します。

AWSLambdaManagedEC2ResourceOperator は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSLambdaManagedEC2ResourceOperator をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 11 月 30 日 08:34 UTC
- 編集日時: 2025 年 11 月 30 日 08:34 UTC
- ARN: arn:aws:iam::aws:policy/AWSLambdaManagedEC2ResourceOperator

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateTags",
        "ec2:AttachNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ManagedResourceOperator" : "scaler.lambda.amazonaws.com"
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:image/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:Owner" : "amazon"
        }
      }
    }
  ]
```

```
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSLambdaMSKExecutionRole

説明: VPC 内の MSK クラスターへのアクセス、VPC 内の ENI の管理 (作成、記述、削除)、および CloudWatch ログへの書き込みに必要なアクセス権限を提供します。

`AWSLambdaMSKExecutionRole` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSLambdaMSKExecutionRole` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 8 月 11 日 17:35 UTC
- 編集日時: 2022 年 8 月 2 日 20:08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaMSKExecutionRole`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSLambdaReplicator

説明: Lambda Replicator に、リージョン間で関数を複製するのに必要な権限を付与します

AWSLambdaReplicator は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 5 月 23 日 17:53 UTC
- 編集日時: 2017 年 12 月 8 日 00:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLambdaReplicator`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSLambdaRole

説明: AWS Lambda サービスロールのデフォルトポリシー。

AWSLambdaRole は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSLambdaRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2015 年 2 月 6 日 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaRole`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSLambdaServiceRolePolicy

説明: Lambda がユーザーに代わって EC2 からマネージドインスタンスを記述および終了できるようにします。

AWSLambdaServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2025 年 11 月 30 日 08:04 UTC
- 編集日時: 2025 年 11 月 30 日 08:04 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSLambdaServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
```

```
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ManagedResourceOperator" : "scaler.lambda.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSLambdaSQSQueueExecutionRole

説明: SQS キューへのメッセージ受信、メッセージ削除、属性の読み取りアクセス、および CloudWatch ログへの書き込み権限を提供します。

`AWSLambdaSQSQueueExecutionRole` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSLambdaSQSQueueExecutionRole` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー

- 作成日時: 2018 年 6 月 14 日 21:50 UTC
- 編集日時: 2018 年 6 月 14 日 21:50 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaSQSQueueExecutionRole`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:ReceiveMessage",
        "sqs:DeleteMessage",
        "sqs:GetQueueAttributes",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSLambdaVPCAccessExecutionRole

説明: VPC 内のリソースにアクセスしながら Lambda 関数を実行するための最低限の権限、つまりネットワークインターフェイスの作成、記述、削除、および CloudWatch Logs への書き込み権限を提供します。

AWSLambdaVPCAccessExecutionRole は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSLambdaVPCAccessExecutionRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2016 年 2 月 11 日 23:15 UTC
- 編集日時: 2024 年 1 月 5 日 22:38 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSLambdaVPCAccessExecutionRole

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSLicenseManagerConsumptionPolicy

説明: ユーザーが使用権限を持っているライセンスで消費するために必要な AWS License Manager API アクションへのアクセスを許可するアクセス許可を提供します。

AWSLicenseManagerConsumptionPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSLicenseManagerConsumptionPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2021 年 8 月 11 日 23:18 UTC
- 編集日時: 2021 年 8 月 11 日 23:18 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSLicenseManagerConsumptionPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "license-manager:CheckoutLicense",
      "license-manager:CheckInLicense",
      "license-manager:ExtendLicenseConsumption",
      "license-manager:GetLicense"
    ],
    "Resource" : "*"
  }
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy

説明: AWS License Manager Linux Subscriptions Service がユーザーに代わってリソースを管理できるようにします。

`AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 12 月 20 日 18:54 UTC
- 編集日時: 2024 年 7 月 8 日 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeRegions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "OrganizationPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:DescribeAccount",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:ListAccountsForParent",
        "organizations:ListRoots",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/LicenseManagerLinuxSubscriptions" : "enabled",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:*"
      ]
    },
    {
      "Sid" : "KMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/LicenseManagerLinuxSubscriptions" : "enabled",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
```

```
          "kms:ViaService" : [
            "secretsmanager.*.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:kms:*:*:key/*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSLicenseManagerMasterAccountRolePolicy

説明: AWS License Manager サービスマスターアカウントロールポリシー

AWSLicenseManagerMasterAccountRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 11 月 26 日 19:03 UTC
- 編集日時: 2022 年 5 月 31 日 20:50 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerMasterAccountRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSLicenseManagerMemberAccountRolePolicy

説明: AWS License Manager サービスメンバーアカウントロールポリシー

`AWSLicenseManagerMemberAccountRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 11 月 26 日 19:04 UTC
- 編集日時: 2019 年 11 月 15 日 22:09 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerMemberAccountRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSLicenseManagerServiceRolePolicy

説明: AWS License Manager サービスのデフォルトロールポリシー

AWSLicenseManagerServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 11 月 26 日 19:02 UTC
- 編集日時: 2025 年 11 月 19 日 18:34 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
    {
      "Sid" : "IAMPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/license-
management.marketplace.amazonaws.com/AWSServiceRoleForMarketplaceLicenseManagement"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "license-management.marketplace.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMPermissionsForCreatingMemberSLR",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:*:iam::*:role/aws-service-role/license-manager.member-
account.amazonaws.com/AWSServiceRoleForAWSLicenseManagerMemberAccountRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "license-manager.member-account.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "S3BucketPermissions1",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-license-manager-service-*"
      ]
    },
    {
```

```
      "Sid" : "S3BucketPermissions2",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "S3ObjectPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-license-manager-service-*"
      ]
    },
    {
      "Sid" : "SNSAccountPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:aws-license-manager-service-*"
      ]
    },
    {
      "Sid" : "SNSTopicPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
```

```
        "ec2:DescribeImages",
        "ec2:DescribeHosts"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SSMPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListInventoryEntries",
        "ssm:GetInventory",
        "ssm:CreateAssociation",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SSMSendCommandPermission",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*::document/AWSLicenseManager-*"
      ]
    },
    {
      "Sid" : "OrganizationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : [
        "*"
      ]
    },
```

```
    {
      "Sid" : "LicenseManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "license-manager:GetServiceSettings",
        "license-manager:GetLicense*",
        "license-manager:UpdateLicenseSpecificationsForResource",
        "license-manager:List*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSLicenseManagerUserSubscriptionsServiceRolePolicy

説明: AWS License Manager User Subscriptions Service がユーザーに代わってリソースを管理できるようにします。

`AWSLicenseManagerUserSubscriptionsServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 7 月 30 日 01:17 UTC
- 編集日時: 2024 年 11 月 8 日 02:54 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DSReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ds:DescribeDirectories",
        "ds:GetAuthorizedApplicationDetails"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetInventory",
        "ssm:GetCommandInvocation",
        "ssm:ListCommandInvocations",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeVpcPeeringConnections"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2WritePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances",
        "ec2:CreateTags"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:productCode" : [
            "bz0vcy31ooqlzk5tsash4r1ik",
            "d44g89hc0gp9jdzm99rznthpw",
            "77yzkpa7kvee1y1tt7wnsdwoc",
            "a8jthu9h8pjsn4b8ylvfl6sfr",
            "7at6der8hnlov1g347e6tdkde",
            "3t0v0vuhvxjzm6m462f9v8iz4",
            "4gs2prcp03ojilgkjx8m3ifh7"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Sid" : "SSMDocumentExecutionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ssm:*::document/AWS-RunPowerShellScript"
      ]
    },
    {
      "Sid" : "SSMInstanceExecutionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSLicenseManager" : "UserSubscriptions"
        }
      }
    },
    {
      "Sid" : "ReadHostedZonePermissions",
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
        "route53:ListResourceRecordSets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ReadSecurityGroupRulePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSecurityGroupRules"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Sid" : "DescribeSubnetsPermissions",
      "Action" : [
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeNetworkInterfacePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ReadSecretPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:license-manager-user-*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSM2ServicePolicy

説明: AWS M2 がユーザーに代わって AWS リソースを管理できるようにします。

AWSM2ServicePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 6 月 7 日 20:26 UTC
- 編集日時: 2022 年 6 月 7 日 20:26 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSM2ServicePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSManagedServices_ContactsServiceRolePolicy

説明: AWS マネージドサービスが AWS リソースのタグの値を読み取ることを許可する

AWSManagedServices_ContactsServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 3 月 23 日 17:07 UTC
- 編集日時: 2023 年 3 月 23 日 17:07 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy

説明: AWS マネージドサービス - 検出コントロールインフラストラクチャを管理するためのポリシー

AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 12 月 19 日 23:11 UTC
- 編集日時: 2022 年 12 月 19 日 23:11 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSManagedServices_EventsServiceRolePolicy

説明: AMS イベントプロセッサ機能を有効にする AWS マネージドサービスポリシー。

AWSManagedServices_EventsServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー

- 作成日時: 2023 年 2 月 7 日 18:41 UTC
- 編集日時: 2023 年 2 月 7 日 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_EventsServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSManagedServices_SelfServiceReporting_ServiceRolePolicy

説明: Amazon の AWS Managed Service のセルフサービスレポート機能でユーザーに代わって AWS Organization のデータを読み取り、組織レベルの集計レポートを有効にする

`AWSManagedServices_SelfServiceReporting_ServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2025 年 1 月 8 日 21:22 UTC
- 編集日時: 2025 年 1 月 8 日 21:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_SelfServiceReporting_ServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSManagedServicesDeploymentToolkitPolicy

説明: AWS マネージドサービスがユーザーに代わってデプロイツールキットを管理できるようにします。

AWSManagedServicesDeploymentToolkitPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー

- 作成日時: 2022 年 6 月 9 日 18:33 UTC
- 編集日時: 2024 年 4 月 4 日 20:41 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServicesDeploymentToolkitPolicy`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSManagementConsoleAdministratorAccess

説明: を設定およびカスタマイズするためのフルアクセスを提供します AWS マネジメントコンソール

AWSManagementConsoleAdministratorAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSManagementConsoleAdministratorAccess をアタッチできます。

ポリシーの詳細

- タイプ: ジョブ機能ポリシー
- 作成日時: 2025 年 8 月 14 日 21:19 UTC

- 編集日時: 2025 年 12 月 10 日 00:04 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/AWSManagementConsoleAdministratorAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "uxc:GetAccountColor",
        "uxc:PutAccountColor",
        "uxc:DeleteAccountColor",
        "ec2:DescribeRegions",
        "notifications:GetFeatureOptInStatus",
        "notifications:AssociateChannel",
        "notifications:AssociateManagedNotificationAccountContact",
        "notifications:AssociateManagedNotificationAdditionalChannel",
        "notifications:CreateEventRule",
        "notifications:CreateNotificationConfiguration",
        "notifications:DeleteEventRule",
        "notifications:DeleteNotificationConfiguration",
        "notifications:DeregisterNotificationHub",
        "notifications:DisableNotificationsAccessForOrganization",
        "notifications:DisassociateChannel",
        "notifications:DisassociateManagedNotificationAccountContact",
        "notifications:DisassociateManagedNotificationAdditionalChannel",
        "notifications:EnableNotificationsAccessForOrganization",
        "notifications:GetEventRule",
        "notifications:GetManagedNotificationChildEvent",
        "notifications:GetManagedNotificationConfiguration",
```

```
        "notifications:GetManagedNotificationEvent",
        "notifications:GetNotificationConfiguration",
        "notifications:GetNotificationEvent",
        "notifications:GetNotificationsAccessForOrganization",
        "notifications:ListChannels",
        "notifications:ListEventRules",
        "notifications:ListManagedNotificationChannelAssociations",
        "notifications:ListManagedNotificationChildEvents",
        "notifications:ListManagedNotificationConfigurations",
        "notifications:ListManagedNotificationEvents",
        "notifications:ListNotificationConfigurations",
        "notifications:ListNotificationEvents",
        "notifications:ListNotificationHubs",
        "notifications:ListTagsForResource",
        "notifications:RegisterNotificationHub",
        "notifications:TagResource",
        "notifications:UntagResource",
        "notifications:UpdateEventRule",
        "notifications:UpdateNotificationConfiguration",
        "cloudshell:CreateEnvironment",
        "cloudshell:CreateSession",
        "cloudshell:GetEnvironmentStatus",
        "cloudshell:DeleteEnvironment",
        "cloudshell:GetFileDownloadUrls",
        "cloudshell:GetFileUploadUrls",
        "cloudshell:DescribeEnvironments",
        "cloudshell:PutCredentials",
        "cloudshell:StartEnvironment",
        "cloudshell:StopEnvironment",
        "cloudshell:ApproveCommand",
        "q:StartConversation",
        "q:SendMessage",
        "q:ListConversations",
        "q:GetConversation",
        "q:PassRequest",
        "resource-explorer-2:AssociateDefaultView",
        "resource-explorer-2:BatchGetView",
        "resource-explorer-2:CreateIndex",
        "resource-explorer-2:CreateView",
        "resource-explorer-2:DeleteIndex",
        "resource-explorer-2:DeleteView",
        "resource-explorer-2:DisassociateDefaultView",
        "resource-explorer-2:GetAccountLevelServiceConfiguration",
        "resource-explorer-2:GetDefaultView",
```

```
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:GetManagedView",
        "resource-explorer-2:GetView",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListIndexesForMembers",
        "resource-explorer-2:ListManagedViews",
        "resource-explorer-2:ListSupportedResourceTypes",
        "resource-explorer-2:ListTagsForResource",
        "resource-explorer-2:ListViews",
        "resource-explorer-2:Search",
        "resource-explorer-2:TagResource",
        "resource-explorer-2:UntagResource",
        "resource-explorer-2:UpdateIndexType",
        "resource-explorer-2:UpdateView",
        "action-recommendations:ListRecommendedActions",
        "account:GetAccountInformation"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSManagementConsoleBasicUserAccess

説明: 管理者以外のユーザーに、重要な AWS マネジメントコンソール 機能とユーザーエクスペリエンス (UX) 機能へのアクセスを許可します。

`AWSManagementConsoleBasicUserAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSManagementConsoleBasicUserAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 8 月 14 日 20:34 UTC
- 編集日時: 2025 年 12 月 10 日 00:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSManagementConsoleBasicUserAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "uxc:GetAccountColor",
        "ec2:DescribeRegions",
        "notifications:GetFeatureOptInStatus",
        "notifications:ListManagedNotificationEvents",
        "notifications:ListNotificationConfigurations",
        "notifications:ListNotificationEvents",
        "notifications:ListNotificationHubs",
        "notifications:GetManagedNotificationChildEvent",
        "notifications:GetManagedNotificationEvent",
        "notifications:GetNotificationEvent",
        "notifications:ListManagedNotificationChildEvents",
        "cloudshell:CreateEnvironment",
        "cloudshell:CreateSession",
        "cloudshell:GetEnvironmentStatus",
        "cloudshell:StartEnvironment",
        "cloudshell:DeleteEnvironment",
        "cloudshell:PutCredentials",
```

```
        "cloudshell:StopEnvironment",
        "cloudshell:ApproveCommand",
        "q:StartConversation",
        "q:SendMessage",
        "q:ListConversations",
        "q:GetConversation",
        "q:PassRequest",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:Search",
        "action-recommendations:ListRecommendedActions",
        "account:GetAccountInformation"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSMarketplaceAmiIngestion

説明: AWS Marketplace が Amazon マシンイメージ (AMIs) をコピーして に一覧表示できるようにする AWS Marketplace

`AWSMarketplaceAmiIngestion` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSMarketplaceAmiIngestion` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 9 月 25 日 20:55 UTC

- 編集日時: 2020 年 9 月 25 日 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceAmiIngestion`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSMarketplaceDeploymentServiceRolePolicy

説明: AWS Marketplace が、サブスクライブする製品の販売者デプロイパラメータを作成および管理できるようにします AWS Marketplace。

AWSMarketplaceDeploymentServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 11 月 15 日 23:34 UTC
- 編集日時: 2023 年 11 月 15 日 23:34 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceDeploymentServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSMarketplaceFullAccess

説明: AWS Marketplace ソフトウェアをサブスクライブおよびサブスクライブ解除する機能を提供し、ユーザーが Marketplace の「ソフトウェア」ページから Marketplace ソフトウェアインスタンスを管理できるようにし、EC2 への管理アクセスを提供します。

`AWSMarketplaceFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSMarketplaceFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 11 日 17:21 UTC
- 編集日時: 2025 年 5 月 7 日 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:*",
        "cloudformation:CreateStack",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:List*",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcs",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:CopyImage",
        "ec2:DeregisterImage",
        "ec2:DescribeSnapshots",
        "ec2:DeleteSnapshot",
        "ec2:CreateImage",
        "ec2:DescribeInstanceStatus",
        "ssm:GetAutomationExecution",
        "ssm:ListDocuments",
        "ssm:DescribeDocument",
        "sns:ListTopics",
        "sns:GetTopicAttributes",
        "sns:CreateTopic",
        "iam:GetRole",
        "iam:GetInstanceProfile",
        "iam:ListRoles",
        "iam:ListInstanceProfiles"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSMarketplaceGetEntitlements

説明: AWS Marketplace エンタイトルメントへの読み取りアクセスを提供します

AWSMarketplaceGetEntitlements は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSMarketplaceGetEntitlements をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 3 月 27 日 19:37 UTC
- 編集日時: 2024 年 4 月 5 日 01:27 UTC
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceGetEntitlements

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSMarketplaceGetEntitlements",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:GetEntitlements"
```

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSMarketplaceImageBuildFullAccess

説明: AWS Marketplace プライベートイメージビルド機能へのフルアクセスを提供します。プライベートイメージを作成することに加えて、イメージにタグを追加したり、EC2 インスタンスを起動および終了したりする許可も付与されます。

`AWSMarketplaceImageBuildFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSMarketplaceImageBuildFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 7 月 31 日 23:29 UTC
- 編集日時: 2022 年 3 月 4 日 17:05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceImageBuildFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSMarketplaceLicenseManagementServiceRolePolicy

説明: ライセンス管理 AWS Marketplace のために が使用または管理する AWS のサービス および リソースへのアクセスを有効にします。

AWSMarketplaceLicenseManagementServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 12 月 3 日 08:33 UTC
- 編集日時: 2020 年 12 月 3 日 08:33 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceLicenseManagementServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSMarketplaceManageSubscriptions

説明: AWS Marketplace ソフトウェアのサブスクライブとサブスクライブ解除を行う機能を提供します。

AWSMarketplaceManageSubscriptions は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSMarketplaceManageSubscriptions をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2025 年 12 月 1 日 00:49 UTC
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceManageSubscriptions

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:Subscribe",
        "aws-marketplace:Unsubscribe"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:CreatePrivateMarketplaceRequests",
        "aws-marketplace:ListPrivateMarketplaceRequests",
        "aws-marketplace:DescribePrivateMarketplaceRequests"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListPrivateListings"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:UpdatePurchaseOrders",
        "aws-marketplace:ListAgreementCharges",
        "aws-marketplace:GetAgreementPaymentRequest",
        "aws-marketplace:ListAgreementPaymentRequests",
        "aws-marketplace:AcceptAgreementPaymentRequest",
        "aws-marketplace:RejectAgreementPaymentRequest"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
```

```
          "aws-marketplace:AgreementType" : [
            "PurchaseAgreement"
          ]
        },
        "Null" : {
          "aws-marketplace:AgreementType" : "false"
        }
      }
    },
    {
      "Sid" : "AWSMarketplaceChangeSetReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:ListChangeSets"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/ChangeSet/*"
    },
    {
      "Sid" : "AWSMarketplaceTokenManagement",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:StartChangeSet"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/AgentTokenContainer/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ChangeSet/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "catalog:ChangeType" : [
            "CreateAgentTokenContainer",
            "RequestExpressPrivateOffer",
            "ExpireToken"
          ]
        }
      }
    },
    {
      "Sid" : "AWSMarketplaceEntityReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListEntities",
        "aws-marketplace:DescribeEntity"
```

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSMarketplaceMeteringFullAccess

説明: AWS Marketplace Metering へのフルアクセスを提供します。

`AWSMarketplaceMeteringFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSMarketplaceMeteringFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2016 年 3 月 17 日 22:39 UTC
- 編集日時: 2016 年 3 月 17 日 22:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceMeteringFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSMarketplaceMeteringRegisterUsage

説明: AWS Marketplace Metering Service を通じてリソースを登録し、使用状況を追跡するアクセス許可を提供します。

`AWSMarketplaceMeteringRegisterUsage` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSMarketplaceMeteringRegisterUsage` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 11 月 21 日 01:17 UTC

- 編集日時: 2019 年 11 月 21 日 01:17 UTC
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceMeteringRegisterUsage

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSMarketplaceProcurementSystemAdminFullAccess

説明: an AWS Marketplace eProcurement 統合のすべての管理アクションへのフルアクセスを提供します。

AWSMarketplaceProcurementSystemAdminFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSMarketplaceProcurementSystemAdminFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 6 月 25 日 13:07 UTC
- 編集日時: 2019 年 6 月 25 日 13:07 UTC
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceProcurementSystemAdminFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:PutProcurementSystemConfiguration",
        "aws-marketplace:DescribeProcurementSystemConfiguration",
        "organizations:Describe*",
        "organizations:List*"
      ],
      "Resource" : [
        "*"
      ]
    }
```

```
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSMarketplacePurchaseOrdersServiceRolePolicy

説明: AWS Marketplace サービスが発注書管理にアクセスできるようにします。

`AWSMarketplacePurchaseOrdersServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 10 月 27 日 15:12 UTC
- 編集日時: 2021 年 10 月 27 日 15:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplacePurchaseOrdersServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowPurchaseOrderActions",
      "Effect" : "Allow",
      "Action" : [
        "purchase-orders:ViewPurchaseOrders",
        "purchase-orders:ModifyPurchaseOrders"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSMarketplaceRead-only

説明: AWS Marketplace サブスクリプションを確認する機能を提供します

`AWSMarketplaceRead-only` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSMarketplaceRead-only` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2025 年 12 月 1 日 00:34 UTC

- ARN: arn:aws:iam::aws:policy/AWSMarketplaceRead-only

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:ListAgreementCharges",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "iam:ListInstanceProfiles",
        "sns:GetTopicAttributes",
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListPrivateMarketplaceRequests",
        "aws-marketplace:DescribePrivateMarketplaceRequests",
        "aws-marketplace:GetAgreementPaymentRequest",
        "aws-marketplace:ListAgreementPaymentRequests"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListPrivateListings"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSMarketplaceResaleAuthorizationServiceRolePolicy

説明: 再販認可 AWS Marketplace のために が使用または管理する AWS のサービス および リソースへのアクセスを有効にします。

`AWSMarketplaceResaleAuthorizationServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2024 年 3 月 5 日 18:47 UTC
- 編集日時: 2025 年 8 月 1 日 15:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceResaleAuthorizationServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowResaleAuthorizationShareActionsRAMCreate",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : [
        "arn:aws:ram:*:*:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ram:RequestedResourceType" : "aws-marketplace:Entity"
        },
        "ArnLike" : {
          "ram:ResourceArn" : "arn:aws:aws-marketplace:*:*:*/ResaleAuthorization/*"
        },
        "Null" : {
          "ram:Principal" : "true"
        }
```

```
      }
    },
    {
      "Sid" : "AllowResaleAuthorizationShareActionsRAMAssociate",
      "Effect" : "Allow",
      "Action" : [
        "ram:AssociateResourceShare"
      ],
      "Resource" : [
        "arn:aws:ram:*:*:*"
      ],
      "Condition" : {
        "Null" : {
          "ram:Principal" : "false"
        },
        "StringEquals" : {
          "ram:ResourceShareName" : "AWSMarketplaceResaleAuthorization"
        }
      }
    },
    {
      "Sid" : "AllowResaleAuthorizationShareActionsRAMAcceptDelete",
      "Effect" : "Allow",
      "Action" : [
        "ram:AcceptResourceShareInvitation",
        "ram:DeleteResourceShare"
      ],
      "Resource" : [
        "arn:aws:ram:*:*:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ram:ResourceShareName" : "AWSMarketplaceResaleAuthorization"
        }
      }
    },
    {
      "Sid" : "AllowResaleAuthorizationShareActionsRAMGet",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShareInvitations",
        "ram:GetResourceShareAssociations"
      ],
      "Resource" : [
```

```
        "arn:aws:ram:*:*:*"
      ]
    },
    {
      "Sid" : "AllowResaleAuthorizationShareActionsMarketplace",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:PutResourcePolicy",
        "aws-marketplace:GetResourcePolicy",
        "aws-marketplace:DeleteResourcePolicy"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:*/ResaleAuthorization/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "ram.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowResaleAuthorizationShareActionsMarketplaceDescribe",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:*/ResaleAuthorization/*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSMarketplaceSellerFullAccess

説明: AWS Marketplace および AMI 管理などの他の AWS サービスに対するすべての販売者オペレーションへのフルアクセスを提供します。

AWSMarketplaceSellerFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSMarketplaceSellerFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 7 月 2 日 20:40 UTC
- 編集日時: 2025 年 12 月 1 日 00:49 UTC
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceSellerFullAccess

ポリシーのバージョン

ポリシーのバージョン: v17 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MarketplaceManagement",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace-management:uploadFiles",
        "aws-marketplace-management:viewReports",
        "aws-marketplace-management:viewSupport",
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:StartChangeSet",
        "aws-marketplace:CancelChangeSet",
        "aws-marketplace:ListEntities",
        "aws-marketplace:DescribeEntity",
        "aws-marketplace:GetSellerDashboard",
```

```
        "aws-marketplace:ListAssessments",
        "aws-marketplace:DescribeAssessment",
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots",
        "ec2:ModifyImageAttribute",
        "ec2:ModifySnapshotAttribute"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AgreementAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:SearchAgreements",
        "aws-marketplace:DescribeAgreement",
        "aws-marketplace:GetAgreementTerms"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws-marketplace:PartyType" : "Proposer"
        },
        "ForAllValues:StringEquals" : {
          "aws-marketplace:AgreementType" : [
            "PurchaseAgreement"
          ]
        }
      }
    },
    {
      "Sid" : "IAMGetRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Sid" : "AssetScanning",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
```

```
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "assets.marketplace.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "VendorInsights",
      "Effect" : "Allow",
      "Action" : [
        "vendor-insights:GetDataSource",
        "vendor-insights:ListDataSources",
        "vendor-insights:ListSecurityProfiles",
        "vendor-insights:GetSecurityProfile",
        "vendor-insights:GetSecurityProfileSnapshot",
        "vendor-insights:ListSecurityProfileSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TagManagement",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:TagResource",
        "aws-marketplace:UntagResource",
        "aws-marketplace:ListTagsForResource"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/*"
    },
    {
      "Sid" : "SellerSettings",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace-management:GetSellerVerificationDetails",
        "aws-marketplace-management:PutSellerVerificationDetails",
        "aws-marketplace-management:GetBankAccountVerificationDetails",
        "aws-marketplace-management:PutBankAccountVerificationDetails",
        "aws-marketplace-management:GetSecondaryUserVerificationDetails",
        "aws-marketplace-management:PutSecondaryUserVerificationDetails",
        "aws-marketplace-management:GetAdditionalSellerNotificationRecipients",
        "aws-marketplace-management:PutAdditionalSellerNotificationRecipients",
        "payments:GetPaymentInstrument",
        "payments:CreatePaymentInstrument",
        "tax:GetTaxInterview",
```

```
        "tax:PutTaxInterview",
        "tax:GetTaxInfoReportingDocument",
        "tax:ListSupplementalTaxRegistrations",
        "tax:PutSupplementalTaxRegistration",
        "tax:DeleteSupplementalTaxRegistration",
        "tax:GetTaxRegistration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Support",
      "Effect" : "Allow",
      "Action" : [
        "support:CreateCase"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ResourcePolicyManagement",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:GetResourcePolicy",
        "aws-marketplace:PutResourcePolicy",
        "aws-marketplace:DeleteResourcePolicy"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/*"
    },
    {
      "Sid" : "CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "resale-authorization.marketplace.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AgreementPaymentRequestAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:SendAgreementPaymentRequest",
        "aws-marketplace:GetAgreementPaymentRequest",
```

```
        "aws-marketplace:ListAgreementPaymentRequests",
        "aws-marketplace:CancelAgreementPaymentRequest"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws-marketplace:PartyType" : "Proposer"
        },
        "ForAllValues:StringEquals" : {
          "aws-marketplace:AgreementType" : [
            "PurchaseAgreement"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSMarketplaceSellerOfferManagement

説明: 販売者にオファーと契約の管理アクティビティへのアクセスを提供します。

AWSMarketplaceSellerOfferManagement は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSMarketplaceSellerOfferManagement をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 11 月 19 日 00:41 UTC

- 編集日時: 2024 年 11 月 19 日 00:41 UTC
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceSellerOfferManagement

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSMarketplaceChangeSetReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:ListChangeSets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSMarketplaceOfferManagement",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:StartChangeSet"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/Offer/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ChangeSet/*"
      ]
    },
    {
      "Sid" : "AWSMarketplaceCreateOfferOnProduct",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:StartChangeSet"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "catalog:ChangeType" : "CreateOfferOnProduct"
        }
      }
    },
    {
      "Sid" : "AWSMarketplaceListEntities",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListEntities"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSMarketplaceEntitiesReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/Offer/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ContainerProduct/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ProfessionalServicesProduct/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/SaaSProduct/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/AmiProduct/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ResaleAuthorization/*"
      ]
    },
    {
      "Sid" : "AWSMarketplaceAgreementsReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:SearchAgreements",
        "aws-marketplace:DescribeAgreement",
        "aws-marketplace:GetAgreementTerms"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws-marketplace:PartyType" : "Proposer"
        },
        "ForAllValues:StringEquals" : {
```

```
          "aws-marketplace:AgreementType" : [
            "PurchaseAgreement"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSMarketplaceSellerProductsFullAccess

説明: AWS Marketplace 管理製品ページや AMI 管理などの他の AWS サービスへのフルアクセスを販売者に提供します。

`AWSMarketplaceSellerProductsFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSMarketplaceSellerProductsFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 7 月 2 日 21:06 UTC
- 編集日時: 2025 年 12 月 1 日 00:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceSellerProductsFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v10 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MarketplaceListAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:ListEntities",
        "aws-marketplace:ListAssessments"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MarketplaceResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:StartChangeSet",
        "aws-marketplace:CancelChangeSet",
        "aws-marketplace:DescribeEntity"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace*/*"
    },
    {
      "Sid" : "MarketplaceAssessmentAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeAssessment"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2ResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
```

```
        "ec2:DescribeSnapshots",
        "ec2:ModifyImageAttribute",
        "ec2:ModifySnapshotAttribute"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetIAMRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Sid" : "IAMPassRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "assets.marketplace.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "VendorInsightsAccess",
      "Effect" : "Allow",
      "Action" : [
        "vendor-insights:GetDataSource",
        "vendor-insights:ListDataSources",
        "vendor-insights:ListSecurityProfiles",
        "vendor-insights:GetSecurityProfile",
        "vendor-insights:GetSecurityProfileSnapshot",
        "vendor-insights:ListSecurityProfileSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TagAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "aws-marketplace:TagResource",
        "aws-marketplace:UntagResource",
        "aws-marketplace:ListTagsForResource"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace*/*"
    },
    {
      "Sid" : "ResourceSharingAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:GetResourcePolicy",
        "aws-marketplace:PutResourcePolicy",
        "aws-marketplace:DeleteResourcePolicy"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace*/*"
    },
    {
      "Sid" : "MarketplaceEphemeralWriteS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-partner-central-marketplace-ephemeral-writeonly-files/
${aws:PrincipalAccount}/*"
      ]
    },
    {
      "Sid" : "LegacyPartnerCentralAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral-account-management:AccessLegacyPartnerCentral"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "partnercentral-account-management:LegacyPartnerCentralRole" :
 "TechnicalStaff"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSMarketplaceSellerProductsReadOnly

説明: 販売者に AWS Marketplace Management Products ページへの読み取り専用アクセスを提供します。

`AWSMarketplaceSellerProductsReadOnly` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSMarketplaceSellerProductsReadOnly` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 7 月 2 日 21:40 UTC
- 編集日時: 2024 年 12 月 10 日 18:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceSellerProductsReadOnly`

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:ListEntities",
        "aws-marketplace:DescribeEntity",
        "aws-marketplace:ListAssessments",
        "aws-marketplace:DescribeAssessment",
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListTagsForResource"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:GetResourcePolicy"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSMcpServiceActionsFullAccess

説明: すべての MCP サービスアクションへのフルアクセスを提供します。このポリシーは、MCP によって実行されたアクションへのアクセスを許可せず、MCP アクション自体のみを許可します。

AWSMcpServiceActionsFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSMcpServiceActionsFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 11 月 21 日 22:49 UTC
- 編集日時: 2025 年 11 月 21 日 22:49 UTC
- ARN: arn:aws:iam::aws:policy/AWSMcpServiceActionsFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowAllMCPServiceActions",
      "Effect" : "Allow",
      "Action" : "*",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:IsMcpServiceAction" : "true"
```

```
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSMediaConnectServicePolicy

説明: MediaConnect が使用または管理する AWS のサービス および リソースへのアクセスを有効にするデフォルトのポリシー。

`AWSMediaConnectServicePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 4 月 3 日 22:11 UTC
- 編集日時: 2025 年 10 月 29 日 21:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMediaConnectServicePolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:UpdateService",
        "ecs:DeleteService",
        "ecs:CreateService",
        "ecs:DescribeServices",
        "ecs:PutAttributes",
        "ecs:DeleteAttributes",
        "ecs:RunTask",
        "ecs:ListTasks",
        "ecs:StartTask",
        "ecs:StopTask",
        "ecs:DescribeTasks",
        "ecs:DescribeContainerInstances",
        "ecs:UpdateContainerInstancesState"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ecs:cluster" : "arn:aws:ecs:*:*:cluster/MediaConnectGateway"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:CreateCluster",
        "ecs:RegisterTaskDefinition"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ecs:UpdateCluster",
        "ecs:UpdateClusterSettings",
        "ecs:ListAttributes",
        "ecs:DescribeClusters",
        "ecs:DeregisterContainerInstance",
        "ecs:ListContainerInstances"
      ],
      "Resource" : "arn:aws:ecs:*:*:cluster/MediaConnectGateway"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:CreateNetworkInterfacePermission"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/created-for-service" : "MediaConnect"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSMediaLiveAnywhereServiceRolePolicy

説明: MediaLive Anywhere がユーザーに代わって AWS リソースを作成および管理できるようにします。

AWSMediaLiveAnywhereServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2025 年 4 月 14 日 22:07 UTC
- 編集日時: 2025 年 4 月 14 日 22:07 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSMediaLiveAnywhereServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/MediaLive"
        }
      }
    },
    {
      "Sid" : "RegisterAnywhereAgentTaskDefinition",
      "Effect" : "Allow",
      "Action" : [
        "ecs:RegisterTaskDefinition"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:task-definition/MediaLiveAnywhereAgent*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/created_by" : "MediaLiveAnywhere"
        }
      }
    },
    {
      "Sid" : "ECSTagResource",
      "Effect" : "Allow",
      "Action" : [
        "ecs:TagResource"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:task-definition/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ecs:CreateAction" : "RegisterTaskDefinition",
          "aws:RequestTag/created_by" : "MediaLiveAnywhere"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "created_by"
        }
      }
    },
    {
      "Sid" : "UpdateAnywhereAgentService",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ecs:UpdateService"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:*"
      ],
      "Condition" : {
        "ArnLike" : {
          "ecs:Cluster" : "arn:aws:ecs:*:*:cluster/MediaLiveAnywhere*",
          "ecs:Task-Definition" : "arn:aws:ecs:*:*:task-definition/
MediaLiveAnywhereAgent*"
        }
      }
    },
    {
      "Sid" : "ECSListTaskDefinitions",
      "Effect" : "Allow",
      "Action" : [
        "ecs:ListTaskDefinitions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DeregisterAnywhereAgentTaskDefinitionOnCleanup",
      "Effect" : "Allow",
      "Action" : [
        "ecs:DeregisterTaskDefinition"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DeleteAnywhereAgentTaskDefinitionsOnCleanup",
      "Effect" : "Allow",
      "Action" : [
        "ecs:DeleteTaskDefinitions"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:task-definition/MediaLiveAnywhereAgent*"
      ]
    },
    {
```

```
      "Sid" : "DeleteAnywhereAgentServiceOnCleanup",
      "Effect" : "Allow",
      "Action" : [
        "ecs:DeleteService"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:service/MediaLiveAnywhere*/MediaLiveAnywhereAgent*"
      ],
      "Condition" : {
        "ArnLike" : {
          "ecs:Cluster" : "arn:aws:ecs:*:*:cluster/MediaLiveAnywhere*"
        }
      }
    },
    {
      "Sid" : "DeregisterContainerInstanceOnCleanup",
      "Effect" : "Allow",
      "Action" : [
        "ecs:ListContainerInstances",
        "ecs:DeregisterContainerInstance"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:cluster/MediaLiveAnywhere*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSMediaTailorServiceRolePolicy

説明: MediaTailor が使用または管理する AWS リソースへのアクセスを有効にする

AWSMediaTailorServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 9 月 17 日 22:27 UTC
- 編集日時: 2021 年 9 月 17 日 22:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMediaTailorServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSMigrationHubDiscoveryAccess

説明: このポリシーは、AWSMigrationHubService に、ユーザーに代わって AWSApplicationDiscoveryService を呼び出す権限を付与します。

`AWSMigrationHubDiscoveryAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSMigrationHubDiscoveryAccess` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2017 年 8 月 14 日 13:30 UTC
- 編集日時: 2020 年 8 月 6 日 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMigrationHubDiscoveryAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSMigrationHubDMSAccess

説明: Database Migration Service が Migration Hub を呼び出すために顧客のアカウントでロールを引き受けるためのポリシー

`AWSMigrationHubDMSAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSMigrationHubDMSAccess` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2017 年 8 月 14 日 14:00 UTC
- 編集日時: 2019 年 10 月 7 日 17:51 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMigrationHubDMSAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSMigrationHubFullAccess

説明: Migration Hub Service への顧客アクセスを提供するマネージドポリシー

`AWSMigrationHubFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSMigrationHubFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 8 月 14 日 14:02 UTC
- 編集日時: 2019 年 6 月 19 日 21:14 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
```

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSMigrationHubOrchestratorConsoleFullAccess

説明: AWS Migration Hub、 AWS Application Discovery Service、Amazon Simple Storage Service、AWS Secrets Manager への制限付きアクセスを提供します。このポリシーは、 AWS Migration Hub Orchestrator サービスへのフルアクセスも許可します。

`AWSMigrationHubOrchestratorConsoleFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSMigrationHubOrchestratorConsoleFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 4 月 20 日 02:26 UTC
- 編集日時: 2023 年 12 月 5 日 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubOrchestratorConsoleFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSMigrationHubOrchestratorInstanceRolePolicy

説明: このポリシーは、S3 からスクリプトをダウンロードしてインスタンスをオーケストレーションしたり、EC2 インスタンス内でシークレット値を取得できるようにするため、サービスの SAP および MGN 移行インスタンスに添付する必要があります。

AWSMigrationHubOrchestratorInstanceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSMigrationHubOrchestratorInstanceRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 4 月 20 日 02:43 UTC
- 編集日時: 2022 年 4 月 20 日 02:43 UTC
- ARN: arn:aws:iam::aws:policy/AWSMigrationHubOrchestratorInstanceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSMigrationHubOrchestratorPlugin

説明: AWS Migration Hub Orchestrator の Amazon Simple Storage Service、 AWS Secrets Manager、プラグイン関連のアクションへの制限付きアクセスを提供します。

`AWSMigrationHubOrchestratorPlugin` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSMigrationHubOrchestratorPlugin` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 4 月 20 日 02:25 UTC
- 編集日時: 2022 年 4 月 20 日 02:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubOrchestratorPlugin`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSMigrationHubOrchestratorServiceRolePolicy

説明: Migration Hub オーケストレーターがオンプレミスのワークロードを移行およびモダナイズするのに必要とする権限を提供します

AWSMigrationHubOrchestratorServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 4 月 20 日 02:24 UTC
- 編集日時: 2024 年 3 月 4 日 18:25 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubOrchestratorServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess

説明: ネットワークブリッジのない環境を使用する場合に必要のない AWS Transit Gateway および EC2 セキュリティグループを除く AWS Migration Hub リファクタリングスペースおよびその他の AWS 関連サービスへのフルアクセスを許可します。このポリシーでは、Lambda AWS と AWS Resource Access Manager に必要なアクセス許可も除外されます。これは、タグに基づいてスコープダウンできるためです。

`AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 4 月 3 日 20:09 UTC

- 編集日時: 2024 年 4 月 11 日 18:16 UTC
- ARN: arn:aws:iam::aws:policy/AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSMigrationHubRefactorSpaces-SSMAutomationPolicy

説明: SSM オートメーションドキュメント AWSRefactorSpaces-CreateResources に渡された IAM サービスロールを使用して、オートメーションの実行に必要な権限を付与します。このポリシーは、自動化の進行状況を追跡するために EC2 タグへの読み取り/書き込みアクセスを許可します。Refactor Spaces 環境のネットワークブリッジが有効になっている場合、環境内の他の Refactor Spaces サービスによるトラフィックを許可するため、オートメーションは環境のセキュリティグループを EC2 インスタンスにも追加します。このポリシーでは、Application Migration Service の起動後アクション SSM パラメータへのアクセスも付与されます。

`AWSMigrationHubRefactorSpaces-SSMAutomationPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSMigrationHubRefactorSpaces-SSMAutomationPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 8 月 10 日 15:08 UTC
- 編集日時: 2023 年 8 月 10 日 15:08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMigrationHubRefactorSpaces-SSMAutomationPolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSMigrationHubRefactorSpacesFullAccess

説明: AWS MigrationHub Refactor Spaces、 AWS MigrationHub Refactor Spaces コンソール機能、およびその他の関連 AWS サービスへのフルアクセスを許可します。ただし、Lambda と AWS Resource Access Manager AWS に必要なアクセス許可は、タグに基づいてスコープダウンできるため除きます。

`AWSMigrationHubRefactorSpacesFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSMigrationHubRefactorSpacesFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 11 月 29 日 07:12 UTC
- 編集日時: 2024 年 4 月 11 日 17:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubRefactorSpacesFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSMigrationHubRefactorSpacesServiceRolePolicy

説明: AWS Migration Hub リファクタリングスペースによって管理または使用される AWS リソースへのアクセスを提供します。

`AWSMigrationHubRefactorSpacesServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 11 月 29 日 06:50 UTC
- 編集日時: 2023 年 7 月 20 日 15:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubRefactorSpacesServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSMigrationHubSMSAccess

説明: Server Migration Service が、Migration Hub を呼び出すために顧客アカウントでロールを引き受けるためのポリシー

AWSMigrationHubSMSAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSMigrationHubSMSAccess をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2017 年 8 月 14 日 13:57 UTC
- 編集日時: 2019 年 10 月 7 日 18:01 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSMigrationHubSMSAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSMigrationHubStrategyCollector

説明: AWS Migration Hub Strategy Recommendations サービスとの通信、サービスに関連する S3 バケットへの読み取り/書き込みアクセス、ログとメトリクスをアップロードするための Amazon API Gateway アクセス AWS、認証情報を取得するための AWS Secrets Manager アクセス、および関連する サービスを許可するアクセス許可を付与します。

`AWSMigrationHubStrategyCollector` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSMigrationHubStrategyCollector` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 10 月 19 日 20:15 UTC
- 編集日時: 2024 年 4 月 1 日 16:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubStrategyCollector`

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSMigrationHubStrategyConsoleFullAccess

説明: AWS Migration Hub Strategy Recommendations サービスへのフルアクセスと、 を介した関連 AWS サービスへのアクセスを許可します AWS マネジメントコンソール。

`AWSMigrationHubStrategyConsoleFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSMigrationHubStrategyConsoleFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 10 月 19 日 20:13 UTC
- 編集日時: 2022 年 11 月 9 日 00:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubStrategyConsoleFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSMigrationHubStrategyServiceRolePolicy

説明: AWS Migration Hub Strategy Recommendations サービスによって使用または管理される AWS リソースへのアクセスを有効にします。

AWSMigrationHubStrategyServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 10 月 19 日 20:02 UTC
- 編集日時: 2021 年 10 月 19 日 20:02 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubStrategyServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSMobileHub_FullAccess

説明: このポリシーは、 AWS Mobile Hub でプロジェクト (および関連する AWS リソース) を作成、削除、変更するアクセス許可をユーザーに付与するために、任意のユーザー、ロール、またはグループにアタッチできます。これには、各 Mobile Hub プロジェクトのサンプルモバイルアプリのソースコードを生成およびダウンロードする許可も含まれます。

AWSMobileHub_FullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSMobileHub_FullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2016 年 1 月 5 日 19:56 UTC
- 編集日時: 2019 年 12 月 19 日 23:15 UTC
- ARN: arn:aws:iam::aws:policy/AWSMobileHub_FullAccess

ポリシーのバージョン

ポリシーのバージョン: v14 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSMobileHub_ReadOnly

説明: このポリシーは、 AWS Mobile Hub でプロジェクトを一覧表示および表示するアクセス許可をユーザーに付与するために、任意のユーザー、ロール、またはグループにアタッチできます。これには、各 Mobile Hub プロジェクトのサンプルモバイルアプリのソースコードを生成およびダウンロードする許可も含まれます。ユーザーは Mobile Hub プロジェクトの設定を変更することはできません。

`AWSMobileHub_ReadOnly` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSMobileHub_ReadOnly` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2016 年 1 月 5 日 19:55 UTC
- 編集日時: 2018 年 7 月 23 日 21:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMobileHub_ReadOnly`

ポリシーのバージョン

ポリシーのバージョン: v10 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSMSKReplicatorExecutionRole

説明: MSK クラスター間でデータをレプリケートする権限を Amazon MSK Replicator に付与します。

`AWSMSKReplicatorExecutionRole` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSMSKReplicatorExecutionRole` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 12 月 6 日 00:07 UTC
- 編集日時: 2024 年 3 月 25 日 21:36 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMSKReplicatorExecutionRole`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSNATGatewayServiceRolePolicy

説明: NAT ゲートウェイの設定と管理のために VPC リソースを管理するアクセス許可を提供します。

AWSNATGatewayServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー

- 作成日時: 2025 年 11 月 14 日 17:19 UTC
- 編集日時: 2025 年 11 月 14 日 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSNATGatewayServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:DescribeAddresses",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSNetworkFirewallFullAccess

説明: AWS Network Firewall サービスへのフルアクセスを許可します。これには、ファイアウォールリソース、ポリシー、ルールグループを作成、設定、管理、削除するアクセス許可が含まれます。さらに、VPC エンドポイント、S3 バケットポリシー、CloudWatch Logs 設定を変更し、Network Firewall およびログ配信サービスのサービスにリンクされたロールを作成するアクセス許可が含まれます。

AWSNetworkFirewallFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSNetworkFirewallFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 6 月 10 日 21:52 UTC
- 編集日時: 2025 年 6 月 10 日 21:52 UTC
- ARN: arn:aws:iam::aws:policy/AWSNetworkFirewallFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "NetworkFirewall",
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:ListAnalysisReports",
```

```
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListFlowOperations",
        "network-firewall:ListRuleGroups",
        "network-firewall:ListTagsForResource",
        "network-firewall:ListTLSInspectionConfigurations",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeFlowOperation",
        "network-firewall:DescribeLoggingConfiguration",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:DescribeRuleGroupMetadata",
        "network-firewall:DescribeTLSInspectionConfiguration",
        "network-firewall:GetAnalysisReportResults",
        "network-firewall:ListFlowOperationResults",
        "network-firewall:TagResource",
        "network-firewall:UntagResource",
        "network-firewall:AssociateFirewallPolicy",
        "network-firewall:AssociateSubnets",
        "network-firewall:CreateFirewall",
        "network-firewall:CreateFirewallPolicy",
        "network-firewall:CreateRuleGroup",
        "network-firewall:CreateTLSInspectionConfiguration",
        "network-firewall:DeleteFirewall",
        "network-firewall:DeleteFirewallPolicy",
        "network-firewall:DeleteResourcePolicy",
        "network-firewall:DeleteRuleGroup",
        "network-firewall:DeleteTLSInspectionConfiguration",
        "network-firewall:DisassociateSubnets",
        "network-firewall:PutResourcePolicy",
        "network-firewall:StartAnalysisReport",
        "network-firewall:StartFlowCapture",
        "network-firewall:StartFlowFlush",
        "network-firewall:UpdateFirewallAnalysisSettings",
        "network-firewall:UpdateFirewallDeleteProtection",
        "network-firewall:UpdateFirewallDescription",
        "network-firewall:UpdateFirewallEncryptionConfiguration",
        "network-firewall:UpdateFirewallPolicy",
        "network-firewall:UpdateFirewallPolicyChangeProtection",
        "network-firewall:UpdateLoggingConfiguration",
        "network-firewall:UpdateRuleGroup",
        "network-firewall:UpdateSubnetChangeProtection",
        "network-firewall:UpdateTLSInspectionConfiguration"
```

```
      ],
      "Resource" : [
        "arn:aws:network-firewall:*:*:*"
      ]
    },
    {
      "Sid" : "NetworkFirewallEC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ec2:GetManagedPrefixListEntries"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "NetworkFirewallCreateVpcEndpoint",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : "arn:aws:ec2:*:*:*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AWSNetworkFirewallManaged" : "true"
        }
      }
    },
    {
      "Sid" : "NetworkFirewallDeleteVpcEndpoints",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "arn:aws:ec2:*:*:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSNetworkFirewallManaged" : "true"
        }
      }
    },
    {
```

```
      "Sid" : "NetworkFirewallLogging",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:GetLogDelivery",
        "logs:ListLogDeliveries",
        "logs:UpdateLogDelivery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "NetworkFirewallLoggingCWL",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups",
        "logs:DescribeResourcePolicies",
        "logs:PutResourcePolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:*"
    },
    {
      "Sid" : "NetworkFirewallLoggingS3",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketPolicy",
        "s3:PutBucketPolicy"
      ],
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "NetworkFirewallLoggingFirehose",
      "Effect" : "Allow",
      "Action" : "firehose:TagDeliveryStream",
      "Resource" : "arn:aws:firehose:*:*:*"
    },
    {
      "Sid" : "NetworkFirewallSLR",
      "Effect" : "Allow",
```

```
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/network-firewall.amazonaws.com/
AWSServiceRoleForNetworkFirewall"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "network-firewall.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "NetworkFirewallLogDeliverySLR",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/delivery.logs.amazonaws.com/
AWSServiceRoleForLogDelivery"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSNetworkFirewallReadOnlyAccess

説明: 、CLI AWS マネジメントコンソール、および SDK 経由で AWS Network Firewall リソースへの読み取り専用アクセスを提供します。 SDKs このポリシーにより、ユーザーはファイアウォール設定、ポリシー、ルールグループ、および関連するリソースを表示およびモニタリングできます。変更を行うことはできません。

AWSNetworkFirewallReadOnlyAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSNetworkFirewallReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 6 月 10 日 21:52 UTC
- 編集日時: 2025 年 6 月 10 日 21:52 UTC
- ARN: arn:aws:iam::aws:policy/AWSNetworkFirewallReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:ListAnalysisReports",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListFlowOperations",
        "network-firewall:ListRuleGroups",
        "network-firewall:ListTagsForResource",
        "network-firewall:ListTLSInspectionConfigurations",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeFlowOperation",
        "network-firewall:DescribeLoggingConfiguration",
```

```
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:DescribeRuleGroupMetadata",
        "network-firewall:DescribeTLSInspectionConfiguration",
        "network-firewall:GetAnalysisReportResults",
        "network-firewall:ListFlowOperationResults"
      ],
      "Resource" : "arn:aws:network-firewall:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:GetLogDelivery",
        "logs:ListLogDeliveries"
      ],
      "Resource" : "arn:aws:logs:*:*:*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSNetworkFirewallServiceRolePolicy

説明: AWSNetworkFirewall がファイアウォールに必要なリソースの作成および管理をできるようにします。

`AWSNetworkFirewallServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 11 月 17 日 17:17 UTC
- 編集日時: 2023 年 3 月 30 日 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSNetworkFirewallServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSNetworkManagerCloudWANServiceRolePolicy

説明: NetworkManager が Core Network に関連するリソースにアクセスできるようにします。

`AWSNetworkManagerCloudWANServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 7 月 12 日 12:17 UTC
- 編集日時: 2022 年 7 月 12 日 12:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSNetworkManagerCloudWANServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTransitGatewayRouteTableAnnouncement",
        "ec2:DeleteTransitGatewayRouteTableAnnouncement",
        "ec2:EnableTransitGatewayRouteTablePropagation",
        "ec2:DisableTransitGatewayRouteTablePropagation"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSNetworkManagerFullAccess

説明: 経由で Amazon NetworkManager へのフルアクセスを提供します AWS マネジメントコンソール。

`AWSNetworkManagerFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSNetworkManagerFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 12 月 3 日 17:37 UTC
- 編集日時: 2019 年 12 月 3 日 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSNetworkManagerFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "networkmanager:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "networkmanager.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSNetworkManagerReadOnlyAccess

説明: 経由で Amazon NetworkManager への読み取り専用アクセスを提供します AWS マネジメントコンソール。

AWSNetworkManagerReadOnlyAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSNetworkManagerReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 12 月 3 日 17:35 UTC
- 編集日時: 2019 年 12 月 3 日 17:35 UTC
- ARN: arn:aws:iam::aws:policy/AWSNetworkManagerReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "networkmanager:Describe*",
        "networkmanager:Get*",
        "networkmanager:List*"
```

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSNetworkManagerServiceRolePolicy

説明: NetworkManager が Global Networks に関連するリソースにアクセスできるようにします

`AWSNetworkManagerServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 12 月 3 日 14:03 UTC
- 編集日時: 2022 年 7 月 27 日 19:41 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSNetworkManagerServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSObservabilityAdminLogsCentralizationServiceRolePolicy

説明: CloudWatch Logs 一元管理のサービスにリンクされたロールのアクセス許可

AWSObservabilityAdminLogsCentralizationServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2025 年 9 月 15 日 14:34 UTC
- 編集日時: 2025 年 9 月 15 日 14:34 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSObservabilityAdminLogsCentralizationServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "logs.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/LogsManaged" : "true"
        },
        "ArnLike" : {
          "kms:EncryptionContext:aws:logs:arn" : "arn:aws:logs:*:*:log-group:*"
        }
      },
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する

- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSObservabilityAdminServiceRolePolicy

説明: Config Configuration Recorder AWS の管理、Config Configuration Aggregator AWS の管理、Config Recorder AWS 機能用の Config Service Linked Role の作成、レコーダー設定データの消費、組織機能の AWS Organizations データの読み取りを行うためのアクセスを提供します。

AWSObservabilityAdminServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2024 年 11 月 27 日 19:36 UTC
- 編集日時: 2024 年 11 月 27 日 19:36 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSObservabilityAdminServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:PutServiceLinkedConfigurationRecorder",
        "config:DeleteServiceLinkedConfigurationRecorder"
      ],
      "Resource" : [
        "arn:aws:config:*:*:configuration-recorder/
AWSConfigurationRecorderForObservabilityAdmin/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:PutConfigurationAggregator",
        "config:DeleteConfigurationAggregator",
        "config:SelectAggregateResourceConfig"
      ],
      "Resource" : [
        "arn:aws:config:*:*:config-aggregator/aws-service-config-aggregator/
observabilityadmin.amazonaws.com/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/config.amazonaws.com/
AWSServiceRoleForConfig"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "config.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/config.amazonaws.com/
AWSServiceRoleForConfig"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "config.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "config.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "observabilityadmin.amazonaws.com",
            "config.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSObservabilityAdminTelemetryEnablementServiceRolePolicy

説明: ログ、メトリクスなどのリソースの AWS Config レコーダー AWS リソースとテレメトリ設定を管理するためのアクセスを提供します。

`AWSObservabilityAdminTelemetryEnablementServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2025 年 8 月 1 日 18:04 UTC
- 編集日時: 2025 年 12 月 2 日 01:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSObservabilityAdminTelemetryEnablementServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TelemetryOperations",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeFlowLogs",
        "ec2:DescribeVpcs",
        "logs:DescribeLogGroups",
        "logs:DescribeResourcePolicies",
        "logs:ListLogGroups"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagOperationForEC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CloudWatchTelemetryRuleManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "ec2:CreateAction" : "CreateFlowLogs"
        },
```

```
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "CloudWatchTelemetryRuleManaged"
        }
      }
    },
    {
      "Sid" : "TagOperationForLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CloudWatchTelemetryRuleManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "CloudWatchTelemetryRuleManaged"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForVPCLogs",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateFlowLogs"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForVPCFlowLogs",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateFlowLogs"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-flow-log/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:RequestTag/CloudWatchTelemetryRuleManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "CloudWatchTelemetryRuleManaged"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForLogs",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteFlowLogs",
        "logs:CreateDelivery",
        "logs:CreateLogGroup",
        "logs:PutResourcePolicy",
        "logs:PutRetentionPolicy",
        "logs:PutDeliveryDestination",
        "logs:PutDeliverySource",
        "logs:CreateLogStream",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CloudWatchTelemetryRuleManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForEKSApiLogs",
      "Effect" : "Allow",
      "Action" : [
        "eks:UpdateClusterConfig"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Bool" : {
          "eks:loggingType/api" : "true"
        }
```

```
      }
    },
    {
      "Sid" : "TelemetryOperationsForEKSAuditLogs",
      "Effect" : "Allow",
      "Action" : [
        "eks:UpdateClusterConfig"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Bool" : {
          "eks:loggingType/audit" : "true"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForEKSAuthenticatorLogs",
      "Effect" : "Allow",
      "Action" : [
        "eks:UpdateClusterConfig"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Bool" : {
          "eks:loggingType/authenticator" : "true"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForEKSControllerManagerLogs",
      "Effect" : "Allow",
      "Action" : [
        "eks:UpdateClusterConfig"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        },
        "Bool" : {
          "eks:loggingType/controllerManager" : "true"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForEKSSchedulerLogs",
      "Effect" : "Allow",
      "Action" : [
        "eks:UpdateClusterConfig"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Bool" : {
          "eks:loggingType/scheduler" : "true"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForWafLoggingConfigurations",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:PutLoggingConfiguration"
      ],
      "Resource" : "arn:aws:wafv2:*:*:regional/webacl/*",
      "Condition" : {
        "ArnLike" : {
          "wafv2:LogDestinationResource" : "arn:aws:logs:*:*:log-group:*"
        },
        "StringEquals" : {
          "wafv2:LogScope" : "CloudwatchTelemetryRuleManaged",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForWafLogDelivery",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "wafv2.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForELB",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AllowVendedLogDeliveryForResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForBedrock",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-agentcore:AllowVendedLogDeliveryForResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForCloudTrailLogs",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateServiceLinkedChannel",
```

```
        "cloudtrail:UpdateServiceLinkedChannel",
        "cloudtrail:DeleteServiceLinkedChannel"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:channel/aws-service-channel/cloudwatch/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForManagedLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:PutResourcePolicy",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:aws/cloudtrail",
        "arn:aws:logs:*:*:log-group:aws/cloudtrail/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "Route53QueryLoggingListOperations",
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:ListResolverQueryLogConfigs",
        "route53resolver:ListResolverQueryLogConfigAssociations"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "Route53QueryLoggingGetOperations",
```

```
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:GetResolverQueryLogConfig",
        "route53resolver:ListTagsForResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CloudWatchTelemetryRuleManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "Route53QueryLoggingConfigCreation",
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:CreateResolverQueryLogConfig",
        "route53resolver:TagResource"
      ],
      "Resource" : "arn:aws:route53resolver:*:*:resolver-query-log-config/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CloudWatchTelemetryRuleManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "Route53QueryLoggingConfigAssociation",
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:AssociateResolverQueryLogConfig"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CloudWatchTelemetryRuleManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForRoute53LogDeliverySLR",
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:*:iam::*:role/aws-service-role/route53resolver.amazonaws.com/
AWSServiceRoleForRoute53Resolver",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "route53resolver.amazonaws.com"
          ],
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "BoolIfExists" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForRoute53LogDelivery",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMOperationsForConfigServiceLinkedRecorder",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/config.amazonaws.com/
AWSServiceRoleForConfig"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "config.amazonaws.com"
          ],
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "BoolIfExists" : {
```

```
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ManagementOperationsForServiceLinkedRecorder",
      "Effect" : "Allow",
      "Action" : [
        "config:PutServiceLinkedConfigurationRecorder",
        "config:DeleteServiceLinkedConfigurationRecorder",
        "config:AssociateResourceTypes",
        "config:DisassociateResourceTypes"
      ],
      "Resource" : [
        "arn:aws:config:*:*:configuration-recorder/
AWSConfigurationRecorderForObservabilityAdmin_TelemetryEnablement/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ReadOperationsForServiceLinkedRecorder",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigurationRecorders"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "config:ConfigurationRecorderServicePrincipal" : [
            "telemetry-enablement.observabilityadmin.amazonaws.com"
          ],
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSOrganizationsFullAccess

説明: AWS Organizations へのフルアクセスを提供します。

AWSOrganizationsFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSOrganizationsFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 11 月 6 日 20:31 UTC
- 編集日時: 2025 年 4 月 22 日 20:37 UTC
- ARN: arn:aws:iam::aws:policy/AWSOrganizationsFullAccess

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
      "Sid" : "AWSOrganizationsFullAccess",
      "Effect" : "Allow",
      "Action" : "organizations:*",
      "Resource" : "*"
    },
    {
      "Sid" : "AWSOrganizationsFullAccessAccount",
      "Effect" : "Allow",
      "Action" : [
        "account:PutAlternateContact",
        "account:DeleteAlternateContact",
        "account:GetAlternateContact",
        "account:GetContactInformation",
        "account:PutContactInformation",
        "account:ListRegions",
        "account:EnableRegion",
        "account:DisableRegion",
        "account:PutAccountName",
        "account:GetAccountInformation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSOrganizationsFullAccessCreateSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "organizations.amazonaws.com"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSOrganizationsReadOnlyAccess

説明: AWS Organizations への読み取り専用アクセスを提供します。

AWSOrganizationsReadOnlyAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSOrganizationsReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 11 月 6 日 20:32 UTC
- 編集日時: 2024 年 6 月 7 日 21:32 UTC
- ARN: arn:aws:iam::aws:policy/AWSOrganizationsReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSOrganizationsServiceTrustPolicy

説明: AWS Organizations が顧客設定を簡素化 AWS のサービス するために承認された他の と信頼を共有できるようにするポリシー。

AWSOrganizationsServiceTrustPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 10 月 10 日 23:04 UTC
- 編集日時: 2017 年 11 月 1 日 06:01 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSOutpostsAuthorizeServerPolicy

説明: このポリシーは、Outpost サーバーをオンプレミスネットワークにインストールする許可を付与します。

AWSOutpostsAuthorizeServerPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSOutpostsAuthorizeServerPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 1 月 4 日 19:23 UTC
- 編集日時: 2023 年 1 月 4 日 19:23 UTC
- ARN: arn:aws:iam::aws:policy/AWSOutpostsAuthorizeServerPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "outposts:StartConnection",
        "outposts:GetConnection"
      ],
```

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSOutpostsServiceRolePolicy

説明: AWS Outposts によって管理される AWS リソースへのアクセスを有効にするサービスリンクロールポリシー

AWSOutpostsServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 11 月 9 日 22:55 UTC
- 編集日時: 2025 年 4 月 17 日 17:37 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSOutpostsServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PrivateConnectivityServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PrivateConnectivityCreateNetworkInterfacePolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:*:ec2:*:*:vpc/*",
        "arn:*:ec2:*:*:subnet/*",
        "arn:*:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "PrivateConnectivityCreateNetworkInterfaceTaggingPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:*:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
```

```
          "aws:TagKeys" : [
            "outposts:private-connectivity-resourceId"
          ]
        }
      }
    },
    {
      "Sid" : "PrivateConnectivityCreateSecurityGroupPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:*:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "PrivateConnectivityCreateSecurityGroupTaggingPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:*:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "outposts:private-connectivity-resourceId"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSPanoramaApplianceRolePolicy

説明: AWS Panorama アプライアンスの AWS IoT ソフトウェアが Amazon CloudWatch にログをアップロードできるようにします。

AWSPanoramaApplianceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSPanoramaApplianceRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 12 月 1 日 13:13 UTC
- 編集日時: 2020 年 12 月 1 日 13:13 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSPanoramaApplianceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSPanoramaApplianceServiceRolePolicy

説明: AWS Panorama アプライアンスが Amazon CloudWatch にログをアップロードし、 AWS Panorama で使用するために作成された Amazon S3 アクセスポイントからオブジェクトを取得できるようにします。

AWSPanoramaApplianceServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSPanoramaApplianceServiceRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2021 年 10 月 20 日 12:14 UTC
- 編集日時: 2024 年 12 月 10 日 20:06 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSPanoramaApplianceServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PanoramaDeviceCreateLogStream",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/panorama_device*:log-stream:*",
        "arn:aws:logs:*:*:log-group:/aws/panorama/devices/*"
      ]
    },
    {
      "Sid" : "PanoramaDeviceCreateLogGroup",
      "Effect" : "Allow",
      "Action" : "logs:CreateLogGroup",
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/panorama_device*",
        "arn:aws:logs:*:*:log-group:/aws/panorama/devices/*"
      ]
    },
    {
      "Sid" : "PanoramaDevicePutMetric",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "PanoramaDeviceMetrics"
```

```
        }
      }
    },
    {
      "Sid" : "PanoramaDeviceS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket",
        "s3:GetObjectVersion"
      ],
      "Resource" : [
        "arn:aws:s3:::*-nodepackage-store-*",
        "arn:aws:s3:::*-application-payload-store-*",
        "arn:aws:s3:*:*:accesspoint/panorama*"
      ],
      "Condition" : {
        "ArnLike" : {
          "s3:DataAccessPointArn" : "arn:aws:s3:*:*:accesspoint/panorama*"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSPanoramaFullAccess

説明: AWS Panorama へのフルアクセスを提供します

AWSPanoramaFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSPanoramaFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 12 月 1 日 13:12 UTC
- 編集日時: 2024 年 12 月 10 日 20:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPanoramaFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "panorama:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "s3:DataAccessPointArn" : "arn:aws:s3:*:*:accesspoint/panorama*"
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret",
        "secretsmanager:ListSecretVersionIds",
        "secretsmanager:PutSecretValue",
        "secretsmanager:UpdateSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:panorama*",
        "arn:aws:secretsmanager:*:*:secret:Panorama*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "panorama.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:Describe*",
        "logs:Get*",
        "logs:List*",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:TestMetricFilter",
        "logs:FilterLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/panorama_device*:log-stream:*",
        "arn:aws:logs:*:*:log-group:/aws/panorama/devices/*"
      ]
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:ListRoles",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "panorama.amazonaws.com"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSPanoramaGreengrassGroupRolePolicy

説明: AWS Panorama アプライアンスの AWS Lambda 関数が Panorama のリソースを管理し、Amazon CloudWatch にログとメトリクスをアップロードし、Panorama で使用するために作成されたバケット内のオブジェクトを管理できるようにします。

AWSPanoramaGreengrassGroupRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSPanoramaGreengrassGroupRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 12 月 1 日 13:10 UTC
- 編集日時: 2021 年 1 月 6 日 19:30 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSPanoramaGreengrassGroupRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSPanoramaSageMakerRolePolicy

説明: Amazon SageMaker が AWS Panorama で使用するために作成されたバケット内のオブジェクトを管理できるようにします。

AWSPanoramaSageMakerRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSPanoramaSageMakerRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 12 月 1 日 13:13 UTC
- 編集日時: 2020 年 12 月 1 日 13:13 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSPanoramaSageMakerRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PanoramaSageMakerS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:GetBucket*"
      ],
      "Resource" : [
        "arn:aws:s3:::*aws-panorama*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSPanoramaServiceLinkedRolePolicy

説明: AWS Panorama が AWS IoT、 AWS Secrets Manager、および AWS Panorama でリソースを管理できるようにします。

`AWSPanoramaServiceLinkedRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 10 月 20 日 12:12 UTC
- 編集日時: 2021 年 10 月 20 日 12:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSPanoramaServiceLinkedRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSPanoramaServiceRolePolicy

説明: AWS Panorama が Amazon S3、 AWS IoT、 AWS IoT GreenGrass、 AWS Lambda、Amazon SageMaker、Amazon CloudWatch Logs のリソースを管理し、サービスロールを AWS IoT、 AWS IoT GreenGrass、Amazon SageMaker に渡すことを許可します。

`AWSPanoramaServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSPanoramaServiceRolePolicy` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 12 月 1 日 13:14 UTC
- 編集日時: 2020 年 12 月 1 日 13:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSPartnerCentralChannelHandshakeApprovalManagement

説明: チャネルハンドシェイク承認管理アクティビティに必要なアクセスを提供します。

AWSPartnerCentralChannelHandshakeApprovalManagement は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSPartnerCentralChannelHandshakeApprovalManagement をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 11 月 19 日 16:34 UTC
- 編集日時: 2025 年 11 月 19 日 16:34 UTC
- ARN: arn:aws:iam::aws:policy/AWSPartnerCentralChannelHandshakeApprovalManagement

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ChannelHandshakeManagement",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:ListChannelHandshakes",
        "partnercentral:AcceptChannelHandshake",
```

```
        "partnercentral:RejectChannelHandshake"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSPartnerCentralChannelManagement

説明: チャネル管理アクティビティに必要なアクセスを提供します。

AWSPartnerCentralChannelManagement は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSPartnerCentralChannelManagement をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 11 月 19 日 16:34 UTC
- 編集日時: 2025 年 12 月 1 日 00:34 UTC
- ARN: arn:aws:iam::aws:policy/AWSPartnerCentralChannelManagement

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ChannelManagement",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:CreateProgramManagementAccount",
        "partnercentral:UpdateProgramManagementAccount",
        "partnercentral:DeleteProgramManagementAccount",
        "partnercentral:ListProgramManagementAccounts",
        "partnercentral:GetProgramManagementAccount",
        "partnercentral:CreateRelationship",
        "partnercentral:UpdateRelationship",
        "partnercentral:DeleteRelationship",
        "partnercentral:GetRelationship",
        "partnercentral:ListRelationships",
        "partnercentral:CreateChannelHandshake",
        "partnercentral:AcceptChannelHandshake",
        "partnercentral:RejectChannelHandshake",
        "partnercentral:CancelChannelHandshake",
        "partnercentral:ListChannelHandshakes"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "ChannelBillingTransferRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/PartnerCentralChannelBillingTransferManagement",
        "arn:aws:iam::*:role/PartnerCentralChannelBillingTransferReadOnly"
      ]
    },
    {
      "Sid" : "TaggingAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:TagResource",
        "partnercentral:UntagResource",
        "partnercentral:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:partnercentral:*:*:catalog/*/program-management-account/*",
        "arn:aws:partnercentral:*:*:catalog/*/channel-handshake/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "LegacyPartnerCentralAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral-account-management:AccessLegacyPartnerCentral"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "partnercentral-account-management:LegacyPartnerCentralRole" : "ChannelUser"
        }
      }
```

```
    },
    {
      "Sid" : "PartnerDashboardAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:GetPartnerDashboard"
      ],
      "Resource" : [
        "arn:aws:partnercentral::*:catalog/AWS/ReportingData/Resell_V1/Dashboard/*"
      ]
    },
    {
      "Sid" : "PartnerResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:ListPartners",
        "partnercentral:GetPartner"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSPartnerCentralFullAccess

説明: AWS Partner Central および関連 へのフルアクセスを提供します AWS のサービス。

AWSPartnerCentralFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSPartnerCentralFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 11 月 18 日 23:33 UTC
- 編集日時: 2025 年 12 月 1 日 00:34 UTC
- ARN: arn:aws:iam::aws:policy/AWSPartnerCentralFullAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PassAWSPartnerCentralRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/PartnerCentralRoleFor*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "partnercentral-account-management.amazonaws.com"
        }
      }
    },
    {
```

```
      "Sid" : "PartnerUserRoleAssociation",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "Partnercentral-account-management:AssociatePartnerUser",
        "Partnercentral-account-management:DisassociatePartnerUser"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSPartnerCentralAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:*"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "VerificationAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:StartVerification",
        "partnercentral:GetVerification"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassAWSPartnerCentralSnapshotJobRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "iam:PassedToService" : "resource-snapshot-job.partnercentral-
selling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "LegacyPartnerCentralAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral-account-management:AccessLegacyPartnerCentral"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PartnerCentralMarketingAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral-account-management:AccessMarketingCentral"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ChannelBillingTransferRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/PartnerCentralChannelBillingTransferManagement",
        "arn:aws:iam::*:role/PartnerCentralChannelBillingTransferReadOnly"
      ]
    },
    {
      "Sid" : "PartnerCentralEphemeralWriteS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::aws-partner-central-marketplace-ephemeral-writeonly-
files/${aws:PrincipalAccount}/*"
    },
    {
      "Sid" : "SupportAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "support:CreateCase",
        "support:DescribeCases",
        "support:AddCommunicationToCase",
        "support:ResolveCase",
        "support:AddAttachmentsToSet",
        "support:DescribeCommunications"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListEntitiesAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListEntities"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeEntityAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace*/Solution/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace*/OfferSet/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace*/Offer/*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSPartnerCentralMarketingManagement

説明: マーケティングアクティビティに必要なアクセスを提供します。

AWSPartnerCentralMarketingManagement は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSPartnerCentralMarketingManagement をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 12 月 1 日 00:34 UTC
- 編集日時: 2025 年 12 月 1 日 00:34 UTC
- ARN: arn:aws:iam::aws:policy/AWSPartnerCentralMarketingManagement

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PartnerCentralMarketingAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral-account-management:AccessMarketingCentral"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "LegacyPartnerCentralAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral-account-management:AccessLegacyPartnerCentral"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "partnercentral-account-management:LegacyPartnerCentralRole" :
"MarketingStaff"
        }
      }
    },
    {
      "Sid" : "PartnerDiscoveryAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:SearchPartnerProfiles",
        "partnercentral:GetPartnerProfile"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PartnerProfileAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:StartProfileUpdateTask",
        "partnercentral:GetProfileUpdateTask",
        "partnercentral:CancelProfileUpdateTask",
        "partnercentral:PutProfileVisibility",
        "partnercentral:GetProfileVisibility"
      ],
      "Resource" : "arn:aws:partnercentral:*:*:catalog/*/partner/*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "PartnerResourceAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:ListPartners",
        "partnercentral:GetPartner"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "PartnerCentralEphemeralWriteS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::aws-partner-central-marketplace-ephemeral-writeonly-
files/${aws:PrincipalAccount}/*"
    },
    {
      "Sid" : "PartnerDashboardAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:GetPartnerDashboard"
      ],
      "Resource" : [
        "arn:aws:partnercentral::*:catalog/AWS/ReportingData/MarketingCampaign_V1/
Dashboard/*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSPartnerCentralOpportunityManagement

説明: 機会管理アクティビティに必要なアクセスを提供します。

AWSPartnerCentralOpportunityManagement は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSPartnerCentralOpportunityManagement をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 11 月 14 日 19:09 UTC
- 編集日時: 2025 年 12 月 1 日 00:49 UTC
- ARN: arn:aws:iam::aws:policy/AWSPartnerCentralOpportunityManagement

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
        "partnercentral:AssignOpportunity",
        "partnercentral:AssociateOpportunity",
        "partnercentral:CreateEngagement",
        "partnercentral:CreateEngagementContext",
        "partnercentral:CreateEngagementInvitation",
        "partnercentral:CreateOpportunity",
        "partnercentral:CreateResourceSnapshot",
        "partnercentral:CreateResourceSnapshotJob",
        "partnercentral:DeleteResourceSnapshotJob",
        "partnercentral:DisassociateOpportunity",
        "partnercentral:GetAwsOpportunitySummary",
        "partnercentral:GetEngagement",
        "partnercentral:GetEngagementInvitation",
        "partnercentral:GetOpportunity",
        "partnercentral:GetResourceSnapshot",
        "partnercentral:GetResourceSnapshotJob",
        "partnercentral:ListEngagementByAcceptingInvitationTasks",
        "partnercentral:ListEngagementFromOpportunityTasks",
        "partnercentral:ListEngagementInvitations",
        "partnercentral:ListEngagementMembers",
        "partnercentral:ListEngagementResourceAssociations",
        "partnercentral:ListEngagements",
        "partnercentral:ListOpportunities",
        "partnercentral:ListOpportunityFromEngagementTasks",
        "partnercentral:ListResourceSnapshotJobs",
        "partnercentral:ListResourceSnapshots",
        "partnercentral:ListSolutions",
        "partnercentral:RejectEngagementInvitation",
        "partnercentral:StartEngagementByAcceptingInvitationTask",
        "partnercentral:StartEngagementFromOpportunityTask",
        "partnercentral:StartOpportunityFromEngagementTask",
        "partnercentral:StartResourceSnapshotJob",
        "partnercentral:StopResourceSnapshotJob",
        "partnercentral:SubmitOpportunity",
        "partnercentral:UpdateEngagementContext",
        "partnercentral:UpdateOpportunity"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "ListingAWSMarketplaceEntities",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListEntities"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSMarketplaceEntityAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace*/Solution/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace*/OfferSet/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace*/Offer/*"
      ]
    },
    {
      "Sid" : "LegacyPartnerCentralAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral-account-management:AccessLegacyPartnerCentral"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "partnercentral-account-management:LegacyPartnerCentralRole" : "AceManager"
        }
      }
    },
    {
      "Sid" : "PartnerDashboardAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:GetPartnerDashboard"
      ],
      "Resource" : [
```

```
        "arn:aws:partnercentral::*:catalog/AWS/ReportingData/Opportunity_V1/Dashboard/
*",
        "arn:aws:partnercentral::*:catalog/AWS/ReportingData/Engagement_V1/Dashboard/*"
      ]
    },
    {
      "Sid" : "CollaborationChannelAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:CreateCollaborationChannelRequest",
        "partnercentral:ListCollaborationChannels",
        "partnercentral:GetCollaborationChannel",
        "partnercentral:CreateCollaborationChannelMembers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PartnerResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:ListPartners",
        "partnercentral:GetPartner"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "TaggingAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:TagResource",
        "partnercentral:UntagResource",
        "partnercentral:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:partnercentral:*:*:catalog/*/opportunity/*",
        "arn:aws:partnercentral:*:*:catalog/*/resource-snapshot-job/*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSPartnerCentralSandboxFullAccess

説明: サンドボックスカタログの開発者テストに必要なアクセスを提供します。

`AWSPartnerCentralSandboxFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSPartnerCentralSandboxFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 11 月 14 日 19:10 UTC
- 編集日時: 2024 年 12 月 10 日 18:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerCentralSandboxFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSPartnerCentralSandboxAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:*"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : "Sandbox"
        }
      }
    },
    {
      "Sid" : "PassAWSPartnerCentralSnapshotJobRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "resource-snapshot-job.partnercentral-
selling.amazonaws.com"
        }
      }
    }
  ]
```

```
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSPartnerCentralSellingResourceSnapshotJobExecutionRolePolicy

説明: ターゲットエンゲージメントでリソースを読み取り、スナップショットを作成するための ResourceSnapshotJob へのアクセスを提供します。

`AWSPartnerCentralSellingResourceSnapshotJobExecutionRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSPartnerCentralSellingResourceSnapshotJobExecutionRolePolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 12 月 10 日 18:21 UTC
- 編集日時: 2024 年 12 月 10 日 18:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerCentralSellingResourceSnapshotJobExecutionRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:CreateResourceSnapshot"
      ],
      "Resource" : [
        "arn:aws:partnercentral:*::catalog/AWS/engagement/*",
        "arn:aws:partnercentral:*::catalog/Sandbox/engagement/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:GetOpportunity"
      ],
      "Resource" : [
        "arn:aws:partnercentral:*:*:catalog/AWS/opportunity/*",
        "arn:aws:partnercentral:*:*:catalog/Sandbox/opportunity/*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSPartnerLedSupportReadOnlyAccess

説明: このポリシーを使用して、 AWS アカウント内のサービスのサービスメタデータを読み取ることができる API への読み取り専用アクセスを許可できます。このポリシーを使用して、Partner-Led Support プログラムのパートナーに、以下のアクセス許可の詳細セクションで指定されたサービスへのアクセスを提供できます。

AWSPartnerLedSupportReadOnlyAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSPartnerLedSupportReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 11 月 22 日 20:06 UTC
- 編集日時: 2024 年 11 月 22 日 20:06 UTC
- ARN: arn:aws:iam::aws:policy/AWSPartnerLedSupportReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
```

```
        "arn:aws:apigateway:*::/account",
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/apis/*/authorizers",
        "arn:aws:apigateway:*::/apis/*/authorizers/*",
        "arn:aws:apigateway:*::/apis/*/deployments",
        "arn:aws:apigateway:*::/apis/*/deployments/*",
        "arn:aws:apigateway:*::/apis/*/integrations",
        "arn:aws:apigateway:*::/apis/*/integrations/*",
        "arn:aws:apigateway:*::/apis/*/integrations/*/integrationresponses",
        "arn:aws:apigateway:*::/apis/*/integrations/*/integrationresponses/*",
        "arn:aws:apigateway:*::/apis/*/models",
        "arn:aws:apigateway:*::/apis/*/models/*",
        "arn:aws:apigateway:*::/apis/*/routes",
        "arn:aws:apigateway:*::/apis/*/routes/*",
        "arn:aws:apigateway:*::/apis/*/routes/*/routeresponses",
        "arn:aws:apigateway:*::/apis/*/routes/*/routeresponses/*",
        "arn:aws:apigateway:*::/apis/*/stages",
        "arn:aws:apigateway:*::/apis/*/stages/*",
        "arn:aws:apigateway:*::/clientcertificates",
        "arn:aws:apigateway:*::/clientcertificates/*",
        "arn:aws:apigateway:*::/domainnames",
        "arn:aws:apigateway:*::/domainnames/*",
        "arn:aws:apigateway:*::/domainnames/*/apimappings",
        "arn:aws:apigateway:*::/domainnames/*/apimappings/*",
        "arn:aws:apigateway:*::/domainnames/*/basepathmappings",
        "arn:aws:apigateway:*::/domainnames/*/basepathmappings/*",
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/restapis/*/authorizers",
        "arn:aws:apigateway:*::/restapis/*/authorizers/*",
        "arn:aws:apigateway:*::/restapis/*/deployments",
        "arn:aws:apigateway:*::/restapis/*/deployments/*",
        "arn:aws:apigateway:*::/restapis/*/models",
        "arn:aws:apigateway:*::/restapis/*/models/*",
        "arn:aws:apigateway:*::/restapis/*/models/*/default_template",
        "arn:aws:apigateway:*::/restapis/*/resources",
        "arn:aws:apigateway:*::/restapis/*/resources/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integration/responses/
*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/responses/*",
        "arn:aws:apigateway:*::/restapis/*/stages/*/sdks/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integration",
```

```
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/usageplans",
        "arn:aws:apigateway:*::/usageplans/*",
        "arn:aws:apigateway:*::/vpclinks",
        "arn:aws:apigateway:*::/vpclinks/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:describeCertificateAuthority",
        "acm-pca:describeCertificateAuthorityAuditReport",
        "acm-pca:getCertificate",
        "acm-pca:getCertificateAuthorityCertificate",
        "acm-pca:getCertificateAuthorityCsr",
        "acm-pca:listCertificateAuthorities",
        "acm-pca:listTags",
        "acm:describeCertificate",
        "acm:getAccountConfiguration",
        "acm:getCertificate",
        "acm:listCertificates",
        "acm:listTagsForCertificate",
        "athena:batchGetNamedQuery",
        "athena:batchGetQueryExecution",
        "athena:getCalculationExecution",
        "athena:getCalculationExecutionStatus",
        "athena:getDataCatalog",
        "athena:getNamedQuery",
        "athena:getNotebookMetadata",
        "athena:getQueryExecution",
        "athena:getQueryRuntimeStatistics",
        "athena:getSession",
        "athena:getSessionStatus",
        "athena:getWorkGroup",
        "athena:listApplicationDPUSizes",
        "athena:listCalculationExecutions",
        "athena:listDataCatalogs",
        "athena:listEngineVersions",
        "athena:listExecutors",
        "athena:listNamedQueries",
        "athena:listNotebookMetadata",
        "athena:listNotebookSessions",
        "athena:listQueryExecutions",
```

```
        "athena:listSessions",
        "athena:listTagsForResource",
        "athena:listWorkGroups",
        "backup-gateway:getGateway",
        "backup-gateway:getHypervisor",
        "backup-gateway:getHypervisorPropertyMappings",
        "backup-gateway:getVirtualMachine",
        "backup-gateway:listGateways",
        "backup-gateway:listHypervisors",
        "backup-gateway:listVirtualMachines",
        "backup:describeBackupJob",
        "backup:describeBackupVault",
        "backup:describeCopyJob",
        "backup:describeFramework",
        "backup:describeGlobalSettings",
        "backup:describeProtectedResource",
        "backup:describeRecoveryPoint",
        "backup:describeRegionSettings",
        "backup:describeReportJob",
        "backup:describeReportPlan",
        "backup:describeRestoreJob",
        "backup:getBackupPlan",
        "backup:getBackupPlanFromJSON",
        "backup:getBackupPlanFromTemplate",
        "backup:getBackupSelection",
        "backup:getBackupVaultAccessPolicy",
        "backup:getBackupVaultNotifications",
        "backup:getLegalHold",
        "backup:getRecoveryPointRestoreMetadata",
        "backup:getRestoreJobMetadata",
        "backup:getRestoreTestingInferredMetadata",
        "backup:getRestoreTestingPlan",
        "backup:getRestoreTestingSelection",
        "backup:getSupportedResourceTypes",
        "backup:listBackupJobs",
        "backup:listBackupPlanTemplates",
        "backup:listBackupPlanVersions",
        "backup:listBackupPlans",
        "backup:listBackupSelections",
        "backup:listBackupVaults",
        "backup:listCopyJobs",
        "backup:listFrameworks",
        "backup:listLegalHolds",
        "backup:listProtectedResources",
```

```
        "backup:listRecoveryPointsByBackupVault",
        "backup:listRecoveryPointsByLegalHold",
        "backup:listRecoveryPointsByResource",
        "backup:listReportJobs",
        "backup:listReportPlans",
        "backup:listRestoreJobs",
        "backup:listRestoreJobsByProtectedResource",
        "backup:listRestoreTestingPlans",
        "backup:listRestoreTestingSelections",
        "backup:listTags",
        "cloudformation:batchDescribeTypeConfigurations",
        "cloudformation:describeAccountLimits",
        "cloudformation:describeChangeSet",
        "cloudformation:describeChangeSetHooks",
        "cloudformation:describePublisher",
        "cloudformation:describeStackEvents",
        "cloudformation:describeStackInstance",
        "cloudformation:describeStackResource",
        "cloudformation:describeStackResources",
        "cloudformation:describeStackSet",
        "cloudformation:describeStackSetOperation",
        "cloudformation:describeStacks",
        "cloudformation:describeType",
        "cloudformation:describeTypeRegistration",
        "cloudformation:estimateTemplateCost",
        "cloudformation:getStackPolicy",
        "cloudformation:getTemplate",
        "cloudformation:getTemplateSummary",
        "cloudformation:listChangeSets",
        "cloudformation:listExports",
        "cloudformation:listImports",
        "cloudformation:listStackInstances",
        "cloudformation:listStackResources",
        "cloudformation:listStackSetOperationResults",
        "cloudformation:listStackSetOperations",
        "cloudformation:listStackSets",
        "cloudformation:listStacks",
        "cloudformation:listTypeRegistrations",
        "cloudformation:listTypeVersions",
        "cloudformation:listTypes",
        "cloudfront:describeFunction",
        "cloudfront:getCachePolicy",
        "cloudfront:getCachePolicyConfig",
        "cloudfront:getCloudFrontOriginAccessIdentity",
```

```
        "cloudfront:getCloudFrontOriginAccessIdentityConfig",
        "cloudfront:getContinuousDeploymentPolicy",
        "cloudfront:getContinuousDeploymentPolicyConfig",
        "cloudfront:getDistribution",
        "cloudfront:getDistributionConfig",
        "cloudfront:getInvalidation",
        "cloudfront:getKeyGroup",
        "cloudfront:getKeyGroupConfig",
        "cloudfront:getMonitoringSubscription",
        "cloudfront:getOriginAccessControl",
        "cloudfront:getOriginAccessControlConfig",
        "cloudfront:getOriginRequestPolicy",
        "cloudfront:getOriginRequestPolicyConfig",
        "cloudfront:getPublicKey",
        "cloudfront:getPublicKeyConfig",
        "cloudfront:getRealtimeLogConfig",
        "cloudfront:getResponseHeadersPolicy",
        "cloudfront:getResponseHeadersPolicyConfig",
        "cloudfront:getStreamingDistribution",
        "cloudfront:getStreamingDistributionConfig",
        "cloudfront:listCachePolicies",
        "cloudfront:listCloudFrontOriginAccessIdentities",
        "cloudfront:listContinuousDeploymentPolicies",
        "cloudfront:listDistributions",
        "cloudfront:listDistributionsByCachePolicyId",
        "cloudfront:listDistributionsByKeyGroup",
        "cloudfront:listDistributionsByOriginRequestPolicyId",
        "cloudfront:listDistributionsByRealtimeLogConfig",
        "cloudfront:listDistributionsByResponseHeadersPolicyId",
        "cloudfront:listDistributionsByWebACLId",
        "cloudfront:listFunctions",
        "cloudfront:listInvalidations",
        "cloudfront:listKeyGroups",
        "cloudfront:listOriginAccessControls",
        "cloudfront:listOriginRequestPolicies",
        "cloudfront:listPublicKeys",
        "cloudfront:listRealtimeLogConfigs",
        "cloudfront:listResponseHeadersPolicies",
        "cloudfront:listStreamingDistributions",
        "cloudtrail:describeTrails",
        "cloudtrail:getEventSelectors",
        "cloudtrail:lookupEvents",
        "cloudwatch:describeAlarmHistory",
        "cloudwatch:describeAlarms",
```

```
        "cloudwatch:describeAlarmsForMetric",
        "cloudwatch:describeAnomalyDetectors",
        "cloudwatch:describeInsightRules",
        "cloudwatch:getDashboard",
        "cloudwatch:getInsightRuleReport",
        "cloudwatch:getMetricData",
        "cloudwatch:getMetricStatistics",
        "cloudwatch:getMetricStream",
        "cloudwatch:listDashboards",
        "cloudwatch:listManagedInsightRules",
        "cloudwatch:listMetricStreams",
        "cloudwatch:listMetrics",
        "codepipeline:getPipeline",
        "codepipeline:getPipelineState",
        "codepipeline:listActionTypes",
        "codepipeline:listPipelineExecutions",
        "codepipeline:listPipelines",
        "cognito-identity:describeIdentityPool",
        "cognito-identity:getIdentityPoolRoles",
        "cognito-identity:listIdentities",
        "cognito-identity:listIdentityPools",
        "cognito-idp:describeIdentityProvider",
        "cognito-idp:describeResourceServer",
        "cognito-idp:describeRiskConfiguration",
        "cognito-idp:describeUserImportJob",
        "cognito-idp:describeUserPool",
        "cognito-idp:describeUserPoolClient",
        "cognito-idp:describeUserPoolDomain",
        "cognito-idp:getGroup",
        "cognito-idp:getUICustomization",
        "cognito-idp:getUserPoolMfaConfig",
        "cognito-idp:listGroups",
        "cognito-idp:listIdentityProviders",
        "cognito-idp:listResourceServers",
        "cognito-idp:listUserImportJobs",
        "cognito-idp:listUserPoolClients",
        "cognito-idp:listUserPools",
        "cognito-sync:describeDataset",
        "cognito-sync:describeIdentityPoolUsage",
        "cognito-sync:describeIdentityUsage",
        "cognito-sync:getCognitoEvents",
        "cognito-sync:getIdentityPoolConfiguration",
        "cognito-sync:listDatasets",
        "cognito-sync:listIdentityPoolUsage",
```

```
        "connect:describeContact",
        "connect:describePhoneNumber",
        "connect:describeQuickConnect",
        "connect:describeUser",
        "connect:getCurrentMetricData",
        "connect:getMetricData",
        "connect:listContactEvaluations",
        "connect:listEvaluationFormVersions",
        "connect:listEvaluationForms",
        "connect:listPhoneNumbersV2",
        "connect:listQuickConnects",
        "connect:listRoutingProfiles",
        "connect:listSecurityProfiles",
        "connect:listUsers",
        "connect:listViewVersions",
        "connect:listViews",
        "directconnect:describeConnectionLoa",
        "directconnect:describeConnections",
        "directconnect:describeConnectionsOnInterconnect",
        "directconnect:describeCustomerMetadata",
        "directconnect:describeDirectConnectGatewayAssociationProposals",
        "directconnect:describeDirectConnectGatewayAssociations",
        "directconnect:describeDirectConnectGatewayAttachments",
        "directconnect:describeDirectConnectGateways",
        "directconnect:describeHostedConnections",
        "directconnect:describeInterconnectLoa",
        "directconnect:describeInterconnects",
        "directconnect:describeLags",
        "directconnect:describeLoa",
        "directconnect:describeLocations",
        "directconnect:describeRouterConfiguration",
        "directconnect:describeVirtualGateways",
        "directconnect:describeVirtualInterfaces",
        "dms:describeAccountAttributes",
        "dms:describeApplicableIndividualAssessments",
        "dms:describeConnections",
        "dms:describeEndpointSettings",
        "dms:describeEndpointTypes",
        "dms:describeEndpoints",
        "dms:describeEventCategories",
        "dms:describeEventSubscriptions",
        "dms:describeEvents",
        "dms:describeFleetAdvisorCollectors",
        "dms:describeFleetAdvisorDatabases",
```

```
        "dms:describeFleetAdvisorLsaAnalysis",
        "dms:describeFleetAdvisorSchemaObjectSummary",
        "dms:describeFleetAdvisorSchemas",
        "dms:describeOrderableReplicationInstances",
        "dms:describePendingMaintenanceActions",
        "dms:describeRefreshSchemasStatus",
        "dms:describeReplicationInstanceTaskLogs",
        "dms:describeReplicationInstances",
        "dms:describeReplicationSubnetGroups",
        "dms:describeReplicationTaskAssessmentResults",
        "dms:describeReplicationTaskAssessmentRuns",
        "dms:describeReplicationTaskIndividualAssessments",
        "dms:describeReplicationTasks",
        "dms:describeSchemas",
        "dms:describeTableStatistics",
        "ds:describeClientAuthenticationSettings",
        "ds:describeConditionalForwarders",
        "ds:describeDirectories",
        "ds:describeDomainControllers",
        "ds:describeEventTopics",
        "ds:describeLDAPSSettings",
        "ds:describeSharedDirectories",
        "ds:describeSnapshots",
        "ds:describeTrusts",
        "ds:getDirectoryLimits",
        "ds:getSnapshotLimits",
        "ds:listIpRoutes",
        "ds:listSchemaExtensions",
        "ds:listTagsForResource",
        "ec2:describeAccountAttributes",
        "ec2:describeAddressTransfers",
        "ec2:describeAddresses",
        "ec2:describeAddressesAttribute",
        "ec2:describeAggregateIdFormat",
        "ec2:describeAvailabilityZones",
        "ec2:describeBundleTasks",
        "ec2:describeByoipCidrs",
        "ec2:describeCapacityReservationFleets",
        "ec2:describeCapacityReservations",
        "ec2:describeCarrierGateways",
        "ec2:describeClassicLinkInstances",
        "ec2:describeClientVpnAuthorizationRules",
        "ec2:describeClientVpnConnections",
        "ec2:describeClientVpnEndpoints",
```

```
        "ec2:describeClientVpnRoutes",
        "ec2:describeClientVpnTargetNetworks",
        "ec2:describeCoipPools",
        "ec2:describeConversionTasks",
        "ec2:describeCustomerGateways",
        "ec2:describeDhcpOptions",
        "ec2:describeEgressOnlyInternetGateways",
        "ec2:describeExportImageTasks",
        "ec2:describeExportTasks",
        "ec2:describeFastLaunchImages",
        "ec2:describeFastSnapshotRestores",
        "ec2:describeFleetHistory",
        "ec2:describeFleetInstances",
        "ec2:describeFleets",
        "ec2:describeFlowLogs",
        "ec2:describeFpgaImageAttribute",
        "ec2:describeFpgaImages",
        "ec2:describeHostReservationOfferings",
        "ec2:describeHostReservations",
        "ec2:describeHosts",
        "ec2:describeIamInstanceProfileAssociations",
        "ec2:describeIdFormat",
        "ec2:describeIdentityIdFormat",
        "ec2:describeImageAttribute",
        "ec2:describeImages",
        "ec2:describeImportImageTasks",
        "ec2:describeImportSnapshotTasks",
        "ec2:describeInstanceAttribute",
        "ec2:describeInstanceCreditSpecifications",
        "ec2:describeInstanceEventNotificationAttributes",
        "ec2:describeInstanceEventWindows",
        "ec2:describeInstanceStatus",
        "ec2:describeInstanceTypeOfferings",
        "ec2:describeInstanceTypes",
        "ec2:describeInstances",
        "ec2:describeInternetGateways",
        "ec2:describeIpamPools",
        "ec2:describeIpamScopes",
        "ec2:describeIpams",
        "ec2:describeIpv6Pools",
        "ec2:describeKeyPairs",
        "ec2:describeLaunchTemplateVersions",
        "ec2:describeLaunchTemplates",
        "ec2:describeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
```

```
        "ec2:describeLocalGatewayRouteTableVpcAssociations",
        "ec2:describeLocalGatewayRouteTables",
        "ec2:describeLocalGatewayVirtualInterfaceGroups",
        "ec2:describeLocalGatewayVirtualInterfaces",
        "ec2:describeLocalGateways",
        "ec2:describeManagedPrefixLists",
        "ec2:describeMovingAddresses",
        "ec2:describeNatGateways",
        "ec2:describeNetworkAcls",
        "ec2:describeNetworkInterfaceAttribute",
        "ec2:describeNetworkInterfaces",
        "ec2:describePlacementGroups",
        "ec2:describePrefixLists",
        "ec2:describePrincipalIdFormat",
        "ec2:describePublicIpv4Pools",
        "ec2:describeRegions",
        "ec2:describeReservedInstances",
        "ec2:describeReservedInstancesListings",
        "ec2:describeReservedInstancesModifications",
        "ec2:describeReservedInstancesOfferings",
        "ec2:describeRouteTables",
        "ec2:describeScheduledInstanceAvailability",
        "ec2:describeScheduledInstances",
        "ec2:describeSecurityGroupReferences",
        "ec2:describeSecurityGroupRules",
        "ec2:describeSecurityGroups",
        "ec2:describeSnapshotAttribute",
        "ec2:describeSnapshotTierStatus",
        "ec2:describeSnapshots",
        "ec2:describeSpotDatafeedSubscription",
        "ec2:describeSpotFleetInstances",
        "ec2:describeSpotFleetRequestHistory",
        "ec2:describeSpotFleetRequests",
        "ec2:describeSpotInstanceRequests",
        "ec2:describeSpotPriceHistory",
        "ec2:describeStaleSecurityGroups",
        "ec2:describeStoreImageTasks",
        "ec2:describeSubnets",
        "ec2:describeTags",
        "ec2:describeTrafficMirrorFilters",
        "ec2:describeTrafficMirrorSessions",
        "ec2:describeTrafficMirrorTargets",
        "ec2:describeTransitGatewayAttachments",
        "ec2:describeTransitGatewayConnectPeers",
```

```
        "ec2:describeTransitGatewayMulticastDomains",
        "ec2:describeTransitGatewayPeeringAttachments",
        "ec2:describeTransitGatewayPolicyTables",
        "ec2:describeTransitGatewayRouteTableAnnouncements",
        "ec2:describeTransitGatewayRouteTables",
        "ec2:describeTransitGatewayVpcAttachments",
        "ec2:describeTransitGateways",
        "ec2:describeVerifiedAccessEndpoints",
        "ec2:describeVerifiedAccessGroups",
        "ec2:describeVerifiedAccessInstances",
        "ec2:describeVerifiedAccessTrustProviders",
        "ec2:describeVolumeAttribute",
        "ec2:describeVolumeStatus",
        "ec2:describeVolumes",
        "ec2:describeVolumesModifications",
        "ec2:describeVpcAttribute",
        "ec2:describeVpcClassicLink",
        "ec2:describeVpcClassicLinkDnsSupport",
        "ec2:describeVpcEndpointConnectionNotifications",
        "ec2:describeVpcEndpointConnections",
        "ec2:describeVpcEndpointServiceConfigurations",
        "ec2:describeVpcEndpointServicePermissions",
        "ec2:describeVpcEndpointServices",
        "ec2:describeVpcEndpoints",
        "ec2:describeVpcPeeringConnections",
        "ec2:describeVpcs",
        "ec2:describeVpnConnections",
        "ec2:describeVpnGateways",
        "ec2:getAssociatedIpv6PoolCidrs",
        "ec2:getCapacityReservationUsage",
        "ec2:getCoipPoolUsage",
        "ec2:getConsoleOutput",
        "ec2:getConsoleScreenshot",
        "ec2:getDefaultCreditSpecification",
        "ec2:getEbsDefaultKmsKeyId",
        "ec2:getEbsEncryptionByDefault",
        "ec2:getGroupsForCapacityReservation",
        "ec2:getHostReservationPurchasePreview",
        "ec2:getInstanceTypesFromInstanceRequirements",
        "ec2:getIpamAddressHistory",
        "ec2:getIpamPoolAllocations",
        "ec2:getIpamPoolCidrs",
        "ec2:getIpamResourceCidrs",
        "ec2:getLaunchTemplateData",
```

```
        "ec2:getManagedPrefixListAssociations",
        "ec2:getManagedPrefixListEntries",
        "ec2:getReservedInstancesExchangeQuote",
        "ec2:getSerialConsoleAccessStatus",
        "ec2:getSpotPlacementScores",
        "ec2:getSubnetCidrReservations",
        "ec2:getTransitGatewayMulticastDomainAssociations",
        "ec2:getTransitGatewayPrefixListReferences",
        "ec2:getVerifiedAccessEndpointPolicy",
        "ec2:getVerifiedAccessGroupPolicy",
        "ec2:listImagesInRecycleBin",
        "ec2:listSnapshotsInRecycleBin",
        "ec2:searchLocalGatewayRoutes",
        "ec2:searchTransitGatewayMulticastGroups",
        "ec2:searchTransitGatewayRoutes",
        "ecs:describeCapacityProviders",
        "ecs:describeClusters",
        "ecs:describeContainerInstances",
        "ecs:describeServices",
        "ecs:describeTaskDefinition",
        "ecs:describeTaskSets",
        "ecs:describeTasks",
        "ecs:getTaskProtection",
        "ecs:listAccountSettings",
        "ecs:listAttributes",
        "ecs:listClusters",
        "ecs:listContainerInstances",
        "ecs:listServices",
        "ecs:listServicesByNamespace",
        "ecs:listTagsForResource",
        "ecs:listTaskDefinitionFamilies",
        "ecs:listTaskDefinitions",
        "ecs:listTasks",
        "eks:describeAccessEntry",
        "eks:describeAddon",
        "eks:describeAddonConfiguration",
        "eks:describeAddonVersions",
        "eks:describeCluster",
        "eks:describeEksAnywhereSubscription",
        "eks:describeFargateProfile",
        "eks:describeIdentityProviderConfig",
        "eks:describeNodegroup",
        "eks:describePodIdentityAssociation",
        "eks:describeUpdate",
```

```
        "eks:listAccessEntries",
        "eks:listAccessPolicies",
        "eks:listAddons",
        "eks:listAssociatedAccessPolicies",
        "eks:listClusters",
        "eks:listEksAnywhereSubscriptions",
        "eks:listFargateProfiles",
        "eks:listIdentityProviderConfigs",
        "eks:listNodegroups",
        "eks:listPodIdentityAssociations",
        "eks:listUpdates",
        "elasticache:describeCacheClusters",
        "elasticache:describeCacheEngineVersions",
        "elasticache:describeCacheParameterGroups",
        "elasticache:describeCacheParameters",
        "elasticache:describeCacheSecurityGroups",
        "elasticache:describeCacheSubnetGroups",
        "elasticache:describeEngineDefaultParameters",
        "elasticache:describeEvents",
        "elasticache:describeGlobalReplicationGroups",
        "elasticache:describeReplicationGroups",
        "elasticache:describeReservedCacheNodes",
        "elasticache:describeReservedCacheNodesOfferings",
        "elasticache:describeServerlessCacheSnapshots",
        "elasticache:describeServerlessCaches",
        "elasticache:describeServiceUpdates",
        "elasticache:describeSnapshots",
        "elasticache:describeUpdateActions",
        "elasticache:describeUserGroups",
        "elasticache:describeUsers",
        "elasticache:listAllowedNodeTypeModifications",
        "elasticache:listTagsForResource",
        "elasticbeanstalk:checkDNSAvailability",
        "elasticbeanstalk:describeAccountAttributes",
        "elasticbeanstalk:describeApplicationVersions",
        "elasticbeanstalk:describeApplications",
        "elasticbeanstalk:describeConfigurationOptions",
        "elasticbeanstalk:describeEnvironmentHealth",
        "elasticbeanstalk:describeEnvironmentManagedActionHistory",
        "elasticbeanstalk:describeEnvironmentManagedActions",
        "elasticbeanstalk:describeEnvironmentResources",
        "elasticbeanstalk:describeEnvironments",
        "elasticbeanstalk:describeEvents",
        "elasticbeanstalk:describeInstancesHealth",
```

```
        "elasticbeanstalk:describePlatformVersion",
        "elasticbeanstalk:listAvailableSolutionStacks",
        "elasticbeanstalk:listPlatformBranches",
        "elasticbeanstalk:listPlatformVersions",
        "elasticbeanstalk:validateConfigurationSettings",
        "elasticfilesystem:describeAccessPoints",
        "elasticfilesystem:describeFileSystemPolicy",
        "elasticfilesystem:describeFileSystems",
        "elasticfilesystem:describeLifecycleConfiguration",
        "elasticfilesystem:describeMountTargetSecurityGroups",
        "elasticfilesystem:describeMountTargets",
        "elasticfilesystem:describeTags",
        "elasticfilesystem:listTagsForResource",
        "elasticloadbalancing:describeAccountLimits",
        "elasticloadbalancing:describeInstanceHealth",
        "elasticloadbalancing:describeListenerCertificates",
        "elasticloadbalancing:describeListeners",
        "elasticloadbalancing:describeLoadBalancerAttributes",
        "elasticloadbalancing:describeLoadBalancerPolicies",
        "elasticloadbalancing:describeLoadBalancerPolicyTypes",
        "elasticloadbalancing:describeLoadBalancers",
        "elasticloadbalancing:describeRules",
        "elasticloadbalancing:describeSSLPolicies",
        "elasticloadbalancing:describeTags",
        "elasticloadbalancing:describeTargetGroupAttributes",
        "elasticloadbalancing:describeTargetGroups",
        "elasticloadbalancing:describeTargetHealth",
        "elasticloadbalancing:describeTrustStoreAssociations",
        "elasticloadbalancing:describeTrustStoreRevocations",
        "elasticloadbalancing:describeTrustStores",
        "emr-containers:describeJobRun",
        "emr-containers:describeJobTemplate",
        "emr-containers:describeManagedEndpoint",
        "emr-containers:describeVirtualCluster",
        "emr-containers:listJobRuns",
        "emr-containers:listJobTemplates",
        "emr-containers:listManagedEndpoints",
        "emr-containers:listVirtualClusters",
        "emr-serverless:getApplication",
        "emr-serverless:getJobRun",
        "emr-serverless:listApplications",
        "es:describeDomain",
        "es:describeDomainAutoTunes",
        "es:describeDomainChangeProgress",
```

```
        "es:describeDomainConfig",
        "es:describeDomains",
        "es:describeDryRunProgress",
        "es:describeElasticsearchDomain",
        "es:describeElasticsearchDomainConfig",
        "es:describeElasticsearchDomains",
        "es:describeInboundConnections",
        "es:describeInstanceTypeLimits",
        "es:describeOutboundConnections",
        "es:describePackages",
        "es:describeReservedInstanceOfferings",
        "es:describeReservedInstances",
        "es:describeVpcEndpoints",
        "es:getCompatibleVersions",
        "es:getPackageVersionHistory",
        "es:getUpgradeHistory",
        "es:getUpgradeStatus",
        "es:listDomainNames",
        "es:listDomainsForPackage",
        "es:listInstanceTypeDetails",
        "es:listPackagesForDomain",
        "es:listScheduledActions",
        "es:listTags",
        "es:listVersions",
        "es:listVpcEndpointAccess",
        "es:listVpcEndpoints",
        "es:listVpcEndpointsForDomain",
        "events:describeApiDestination",
        "events:describeArchive",
        "events:describeConnection",
        "events:describeEndpoint",
        "events:describeEventBus",
        "events:describeEventSource",
        "events:describePartnerEventSource",
        "events:describeReplay",
        "events:describeRule",
        "events:listApiDestinations",
        "events:listArchives",
        "events:listConnections",
        "events:listEndpoints",
        "events:listEventBuses",
        "events:listEventSources",
        "events:listPartnerEventSourceAccounts",
        "events:listPartnerEventSources",
```

```
        "events:listReplays",
        "events:listRuleNamesByTarget",
        "events:listRules",
        "events:listTargetsByRule",
        "events:testEventPattern",
        "fsx:describeBackups",
        "fsx:describeDataRepositoryAssociations",
        "fsx:describeDataRepositoryTasks",
        "fsx:describeFileCaches",
        "fsx:describeFileSystems",
        "fsx:describeSnapshots",
        "fsx:describeStorageVirtualMachines",
        "fsx:describeVolumes",
        "fsx:listTagsForResource",
        "glue:batchGetBlueprints",
        "glue:batchGetCrawlers",
        "glue:batchGetDevEndpoints",
        "glue:batchGetJobs",
        "glue:batchGetPartition",
        "glue:batchGetTriggers",
        "glue:batchGetWorkflows",
        "glue:checkSchemaVersionValidity",
        "glue:getBlueprint",
        "glue:getBlueprintRun",
        "glue:getBlueprintRuns",
        "glue:getCatalogImportStatus",
        "glue:getClassifier",
        "glue:getClassifiers",
        "glue:getColumnStatisticsForPartition",
        "glue:getColumnStatisticsForTable",
        "glue:getCrawler",
        "glue:getCrawlerMetrics",
        "glue:getCrawlers",
        "glue:getCustomEntityType",
        "glue:getDataQualityResult",
        "glue:getDataQualityRuleRecommendationRun",
        "glue:getDataQualityRuleset",
        "glue:getDataQualityRulesetEvaluationRun",
        "glue:getDatabase",
        "glue:getDatabases",
        "glue:getDataflowGraph",
        "glue:getDevEndpoint",
        "glue:getDevEndpoints",
        "glue:getJob",
```

```
        "glue:getJobRun",
        "glue:getJobRuns",
        "glue:getJobs",
        "glue:getMLTaskRun",
        "glue:getMLTaskRuns",
        "glue:getMLTransform",
        "glue:getMLTransforms",
        "glue:getMapping",
        "glue:getPartition",
        "glue:getPartitionIndexes",
        "glue:getPartitions",
        "glue:getRegistry",
        "glue:getResourcePolicies",
        "glue:getResourcePolicy",
        "glue:getSchema",
        "glue:getSchemaByDefinition",
        "glue:getSchemaVersion",
        "glue:getSchemaVersionsDiff",
        "glue:getSession",
        "glue:getStatement",
        "glue:getTable",
        "glue:getTableVersions",
        "glue:getTables",
        "glue:getTrigger",
        "glue:getTriggers",
        "glue:getUserDefinedFunction",
        "glue:getUserDefinedFunctions",
        "glue:getWorkflow",
        "glue:getWorkflowRun",
        "glue:getWorkflowRuns",
        "glue:listCrawlers",
        "glue:listCrawls",
        "glue:listDataQualityResults",
        "glue:listDataQualityRuleRecommendationRuns",
        "glue:listDataQualityRulesetEvaluationRuns",
        "glue:listDataQualityRulesets",
        "glue:listDevEndpoints",
        "glue:listMLTransforms",
        "glue:listRegistries",
        "glue:listSchemaVersions",
        "glue:listSchemas",
        "glue:listSessions",
        "glue:listStatements",
        "glue:querySchemaVersionMetadata",
```

```
        "guardduty:getFindings",
        "guardduty:listDetectors",
        "guardduty:listFindings",
        "guardduty:listIPSets",
        "guardduty:listThreatIntelSets",
        "iam:getAccessKeyLastUsed",
        "iam:getAccountAuthorizationDetails",
        "iam:getAccountPasswordPolicy",
        "iam:getAccountSummary",
        "iam:getContextKeysForCustomPolicy",
        "iam:getContextKeysForPrincipalPolicy",
        "iam:getCredentialReport",
        "iam:getGroup",
        "iam:getGroupPolicy",
        "iam:getInstanceProfile",
        "iam:getLoginProfile",
        "iam:getOpenIDConnectProvider",
        "iam:getPolicy",
        "iam:getPolicyVersion",
        "iam:getRole",
        "iam:getRolePolicy",
        "iam:getSAMLProvider",
        "iam:getSSHPublicKey",
        "iam:getServerCertificate",
        "iam:getServiceLinkedRoleDeletionStatus",
        "iam:getUser",
        "iam:getUserPolicy",
        "iam:listAccessKeys",
        "iam:listAccountAliases",
        "iam:listAttachedGroupPolicies",
        "iam:listAttachedRolePolicies",
        "iam:listAttachedUserPolicies",
        "iam:listEntitiesForPolicy",
        "iam:listGroupPolicies",
        "iam:listGroups",
        "iam:listGroupsForUser",
        "iam:listInstanceProfiles",
        "iam:listInstanceProfilesForRole",
        "iam:listMFADevices",
        "iam:listOpenIDConnectProviders",
        "iam:listPolicies",
        "iam:listPolicyVersions",
        "iam:listRolePolicies",
        "iam:listRoles",
```

```
        "iam:listSAMLProviders",
        "iam:listSSHPublicKeys",
        "iam:listServerCertificates",
        "iam:listSigningCertificates",
        "iam:listUserPolicies",
        "iam:listUsers",
        "iam:listVirtualMFADevices",
        "kafka:describeCluster",
        "kafka:describeClusterOperation",
        "kafka:describeClusterOperationV2",
        "kafka:describeClusterV2",
        "kafka:describeConfiguration",
        "kafka:describeConfigurationRevision",
        "kafka:describeReplicator",
        "kafka:describeVpcConnection",
        "kafka:getBootstrapBrokers",
        "kafka:getClusterPolicy",
        "kafka:listClientVpcConnections",
        "kafka:listClusterOperations",
        "kafka:listClusterOperationsV2",
        "kafka:listClusters",
        "kafka:listClustersV2",
        "kafka:listConfigurationRevisions",
        "kafka:listConfigurations",
        "kafka:listNodes",
        "kafka:listReplicators",
        "kafka:listScramSecrets",
        "kafka:listVpcConnections",
        "kafkaconnect:describeConnector",
        "kafkaconnect:describeCustomPlugin",
        "kafkaconnect:describeWorkerConfiguration",
        "kafkaconnect:listConnectors",
        "kafkaconnect:listCustomPlugins",
        "kafkaconnect:listWorkerConfigurations",
        "lambda:getAccountSettings",
        "lambda:getAlias",
        "lambda:getCodeSigningConfig",
        "lambda:getEventSourceMapping",
        "lambda:getFunction",
        "lambda:getFunctionCodeSigningConfig",
        "lambda:getFunctionConcurrency",
        "lambda:getFunctionConfiguration",
        "lambda:getFunctionEventInvokeConfig",
        "lambda:getFunctionUrlConfig",
```

```
        "lambda:getLayerVersion",
        "lambda:getLayerVersionPolicy",
        "lambda:getPolicy",
        "lambda:getProvisionedConcurrencyConfig",
        "lambda:getRuntimeManagementConfig",
        "lambda:listAliases",
        "lambda:listCodeSigningConfigs",
        "lambda:listEventSourceMappings",
        "lambda:listFunctionEventInvokeConfigs",
        "lambda:listFunctionUrlConfigs",
        "lambda:listFunctions",
        "lambda:listFunctionsByCodeSigningConfig",
        "lambda:listLayerVersions",
        "lambda:listLayers",
        "lambda:listProvisionedConcurrencyConfigs",
        "lambda:listVersionsByFunction",
        "logs:describeExportTasks",
        "logs:describeLogGroups",
        "logs:describeLogStreams",
        "logs:describeMetricFilters",
        "logs:describeSubscriptionFilters",
        "medialive:listChannels",
        "medialive:listInputSecurityGroups",
        "medialive:listInputs",
        "mobiletargeting:getAdmChannel",
        "mobiletargeting:getApnsChannel",
        "mobiletargeting:getApnsSandboxChannel",
        "mobiletargeting:getApnsVoipChannel",
        "mobiletargeting:getApnsVoipSandboxChannel",
        "mobiletargeting:getApplicationSettings",
        "mobiletargeting:getApps",
        "mobiletargeting:getBaiduChannel",
        "mobiletargeting:getCampaign",
        "mobiletargeting:getCampaignActivities",
        "mobiletargeting:getCampaignVersions",
        "mobiletargeting:getCampaigns",
        "mobiletargeting:getEmailChannel",
        "mobiletargeting:getEventStream",
        "mobiletargeting:getExportJobs",
        "mobiletargeting:getGcmChannel",
        "mobiletargeting:getImportJobs",
        "mobiletargeting:getJourney",
        "mobiletargeting:getJourneyExecutionActivityMetrics",
        "mobiletargeting:getJourneyExecutionMetrics",
```

```
        "mobiletargeting:getJourneyRunExecutionActivityMetrics",
        "mobiletargeting:getJourneyRunExecutionMetrics",
        "mobiletargeting:getJourneyRuns",
        "mobiletargeting:getSegment",
        "mobiletargeting:getSegmentImportJobs",
        "mobiletargeting:getSegmentVersions",
        "mobiletargeting:getSegments",
        "mobiletargeting:getSmsChannel",
        "mobiletargeting:listJourneys",
        "pipes:listPipes",
        "polly:describeVoices",
        "polly:listLexicons",
        "quicksight:describeAccountCustomization",
        "quicksight:describeAccountSettings",
        "quicksight:describeAccountSubscription",
        "quicksight:describeAnalysis",
        "quicksight:describeAnalysisPermissions",
        "quicksight:describeDashboard",
        "quicksight:describeDashboardPermissions",
        "quicksight:describeDataSet",
        "quicksight:describeDataSetRefreshProperties",
        "quicksight:describeDataSource",
        "quicksight:describeFolder",
        "quicksight:describeFolderPermissions",
        "quicksight:describeFolderResolvedPermissions",
        "quicksight:describeGroup",
        "quicksight:describeGroupMembership",
        "quicksight:describeIAMPolicyAssignment",
        "quicksight:describeIngestion",
        "quicksight:describeIpRestriction",
        "quicksight:describeNamespace",
        "quicksight:describeRefreshSchedule",
        "quicksight:describeTemplate",
        "quicksight:describeTemplateAlias",
        "quicksight:describeTemplatePermissions",
        "quicksight:describeTheme",
        "quicksight:describeThemeAlias",
        "quicksight:describeThemePermissions",
        "quicksight:describeTopic",
        "quicksight:describeTopicRefresh",
        "quicksight:describeTopicRefreshSchedule",
        "quicksight:describeUser",
        "quicksight:describeVPCConnection",
        "quicksight:listAnalyses",
```

```
        "quicksight:listDashboardVersions",
        "quicksight:listDashboards",
        "quicksight:listDataSets",
        "quicksight:listDataSources",
        "quicksight:listFolderMembers",
        "quicksight:listFolders",
        "quicksight:listGroupMemberships",
        "quicksight:listGroups",
        "quicksight:listIAMPolicyAssignments",
        "quicksight:listIAMPolicyAssignmentsForUser",
        "quicksight:listIngestions",
        "quicksight:listNamespaces",
        "quicksight:listRefreshSchedules",
        "quicksight:listTemplateAliases",
        "quicksight:listTemplateVersions",
        "quicksight:listTemplates",
        "quicksight:listThemeAliases",
        "quicksight:listThemeVersions",
        "quicksight:listThemes",
        "quicksight:listTopicRefreshSchedules",
        "quicksight:listTopics",
        "quicksight:listUserGroups",
        "quicksight:listUsers",
        "quicksight:listVPCConnections",
        "quicksight:searchAnalyses",
        "quicksight:searchDashboards",
        "quicksight:searchDataSets",
        "quicksight:searchDataSources",
        "quicksight:searchFolders",
        "quicksight:searchGroups",
        "rds:describeAccountAttributes",
        "rds:describeBlueGreenDeployments",
        "rds:describeCertificates",
        "rds:describeDBClusterEndpoints",
        "rds:describeDBClusterParameterGroups",
        "rds:describeDBClusterParameters",
        "rds:describeDBClusterSnapshots",
        "rds:describeDBClusters",
        "rds:describeDBEngineVersions",
        "rds:describeDBInstanceAutomatedBackups",
        "rds:describeDBInstances",
        "rds:describeDBLogFiles",
        "rds:describeDBParameterGroups",
        "rds:describeDBParameters",
```

```
        "rds:describeDBSecurityGroups",
        "rds:describeDBSnapshotAttributes",
        "rds:describeDBSnapshots",
        "rds:describeDBSubnetGroups",
        "rds:describeEngineDefaultClusterParameters",
        "rds:describeEngineDefaultParameters",
        "rds:describeEventCategories",
        "rds:describeEventSubscriptions",
        "rds:describeEvents",
        "rds:describeExportTasks",
        "rds:describeGlobalClusters",
        "rds:describeIntegrations",
        "rds:describeOptionGroupOptions",
        "rds:describeOptionGroups",
        "rds:describeOrderableDBInstanceOptions",
        "rds:describePendingMaintenanceActions",
        "rds:describeReservedDBInstances",
        "rds:describeReservedDBInstancesOfferings",
        "rds:describeSourceRegions",
        "rds:describeValidDBInstanceModifications",
        "rds:listTagsForResource",
        "redshift-data:describeStatement",
        "redshift-data:listStatements",
        "redshift-serverless:getEndpointAccess",
        "redshift-serverless:getNamespace",
        "redshift-serverless:getRecoveryPoint",
        "redshift-serverless:getSnapshot",
        "redshift-serverless:getTableRestoreStatus",
        "redshift-serverless:getUsageLimit",
        "redshift-serverless:getWorkgroup",
        "redshift-serverless:listEndpointAccess",
        "redshift-serverless:listNamespaces",
        "redshift-serverless:listRecoveryPoints",
        "redshift-serverless:listSnapshots",
        "redshift-serverless:listTableRestoreStatus",
        "redshift-serverless:listUsageLimits",
        "redshift-serverless:listWorkgroups",
        "redshift:describeClusterParameterGroups",
        "redshift:describeClusterParameters",
        "redshift:describeClusterSecurityGroups",
        "redshift:describeClusterSnapshots",
        "redshift:describeClusterSubnetGroups",
        "redshift:describeClusterVersions",
        "redshift:describeClusters",
```

```
        "redshift:describeDataShares",
        "redshift:describeDataSharesForConsumer",
        "redshift:describeDataSharesForProducer",
        "redshift:describeDefaultClusterParameters",
        "redshift:describeEventCategories",
        "redshift:describeEventSubscriptions",
        "redshift:describeEvents",
        "redshift:describeHsmClientCertificates",
        "redshift:describeHsmConfigurations",
        "redshift:describeLoggingStatus",
        "redshift:describeOrderableClusterOptions",
        "redshift:describeReservedNodeOfferings",
        "redshift:describeReservedNodes",
        "redshift:describeResize",
        "redshift:describeSnapshotCopyGrants",
        "redshift:describeStorage",
        "redshift:describeTableRestoreStatus",
        "redshift:describeTags",
        "route53-recovery-cluster:getRoutingControlState",
        "route53-recovery-cluster:listRoutingControls",
        "route53-recovery-control-config:describeControlPanel",
        "route53-recovery-control-config:describeRoutingControl",
        "route53-recovery-control-config:describeSafetyRule",
        "route53-recovery-control-config:listControlPanels",
        "route53-recovery-control-config:listRoutingControls",
        "route53-recovery-control-config:listSafetyRules",
        "route53-recovery-readiness:getCell",
        "route53-recovery-readiness:getCellReadinessSummary",
        "route53-recovery-readiness:getReadinessCheck",
        "route53-recovery-readiness:getReadinessCheckResourceStatus",
        "route53-recovery-readiness:getReadinessCheckStatus",
        "route53-recovery-readiness:getRecoveryGroup",
        "route53-recovery-readiness:getRecoveryGroupReadinessSummary",
        "route53-recovery-readiness:listCells",
        "route53-recovery-readiness:listReadinessChecks",
        "route53-recovery-readiness:listRecoveryGroups",
        "route53-recovery-readiness:listResourceSets",
        "route53:getAccountLimit",
        "route53:getChange",
        "route53:getCheckerIpRanges",
        "route53:getDNSSEC",
        "route53:getGeoLocation",
        "route53:getHealthCheck",
        "route53:getHealthCheckCount",
```

```
        "route53:getHealthCheckLastFailureReason",
        "route53:getHealthCheckStatus",
        "route53:getHostedZone",
        "route53:getHostedZoneCount",
        "route53:getHostedZoneLimit",
        "route53:getQueryLoggingConfig",
        "route53:getReusableDelegationSet",
        "route53:getTrafficPolicy",
        "route53:getTrafficPolicyInstance",
        "route53:getTrafficPolicyInstanceCount",
        "route53:listCidrBlocks",
        "route53:listCidrCollections",
        "route53:listCidrLocations",
        "route53:listGeoLocations",
        "route53:listHealthChecks",
        "route53:listHostedZones",
        "route53:listHostedZonesByName",
        "route53:listHostedZonesByVpc",
        "route53:listQueryLoggingConfigs",
        "route53:listResourceRecordSets",
        "route53:listReusableDelegationSets",
        "route53:listTrafficPolicies",
        "route53:listTrafficPolicyInstances",
        "route53:listTrafficPolicyInstancesByHostedZone",
        "route53:listTrafficPolicyInstancesByPolicy",
        "route53:listTrafficPolicyVersions",
        "route53:listVPCAssociationAuthorizations",
        "route53domains:checkDomainAvailability",
        "route53domains:getContactReachabilityStatus",
        "route53domains:getDomainDetail",
        "route53domains:getOperationDetail",
        "route53domains:listDomains",
        "route53domains:listOperations",
        "route53domains:listPrices",
        "route53domains:listTagsForDomain",
        "route53domains:viewBilling",
        "route53resolver:getFirewallConfig",
        "route53resolver:getFirewallDomainList",
        "route53resolver:getFirewallRuleGroup",
        "route53resolver:getFirewallRuleGroupAssociation",
        "route53resolver:getFirewallRuleGroupPolicy",
        "route53resolver:getOutpostResolver",
        "route53resolver:getResolverDnssecConfig",
        "route53resolver:getResolverQueryLogConfig",
```

```
        "route53resolver:getResolverQueryLogConfigAssociation",
        "route53resolver:getResolverQueryLogConfigPolicy",
        "route53resolver:getResolverRule",
        "route53resolver:getResolverRuleAssociation",
        "route53resolver:getResolverRulePolicy",
        "route53resolver:listFirewallConfigs",
        "route53resolver:listFirewallDomainLists",
        "route53resolver:listFirewallDomains",
        "route53resolver:listFirewallRuleGroupAssociations",
        "route53resolver:listFirewallRuleGroups",
        "route53resolver:listFirewallRules",
        "route53resolver:listOutpostResolvers",
        "route53resolver:listResolverConfigs",
        "route53resolver:listResolverDnssecConfigs",
        "route53resolver:listResolverEndpointIpAddresses",
        "route53resolver:listResolverEndpoints",
        "route53resolver:listResolverQueryLogConfigAssociations",
        "route53resolver:listResolverQueryLogConfigs",
        "route53resolver:listResolverRuleAssociations",
        "route53resolver:listResolverRules",
        "route53resolver:listTagsForResource",
        "s3:describeJob",
        "s3:describeMultiRegionAccessPointOperation",
        "s3:getAccelerateConfiguration",
        "s3:getAccessPoint",
        "s3:getAccessPointConfigurationForObjectLambda",
        "s3:getAccessPointForObjectLambda",
        "s3:getAccessPointPolicy",
        "s3:getAccessPointPolicyForObjectLambda",
        "s3:getAccessPointPolicyStatus",
        "s3:getAccessPointPolicyStatusForObjectLambda",
        "s3:getAccountPublicAccessBlock",
        "s3:getAnalyticsConfiguration",
        "s3:getBucketAcl",
        "s3:getBucketCORS",
        "s3:getBucketLocation",
        "s3:getBucketLogging",
        "s3:getBucketNotification",
        "s3:getBucketObjectLockConfiguration",
        "s3:getBucketOwnershipControls",
        "s3:getBucketPolicy",
        "s3:getBucketPolicyStatus",
        "s3:getBucketPublicAccessBlock",
        "s3:getBucketRequestPayment",
```

```
        "s3:getBucketVersioning",
        "s3:getBucketWebsite",
        "s3:getEncryptionConfiguration",
        "s3:getIntelligentTieringConfiguration",
        "s3:getInventoryConfiguration",
        "s3:getLifecycleConfiguration",
        "s3:getMetricsConfiguration",
        "s3:getMultiRegionAccessPoint",
        "s3:getMultiRegionAccessPointPolicy",
        "s3:getMultiRegionAccessPointPolicyStatus",
        "s3:getMultiRegionAccessPointRoutes",
        "s3:getObjectLegalHold",
        "s3:getObjectRetention",
        "s3:getReplicationConfiguration",
        "s3:getStorageLensConfiguration",
        "s3:listAccessPoints",
        "s3:listAccessPointsForObjectLambda",
        "s3:listAllMyBuckets",
        "s3:listBucket",
        "s3:listBucketMultipartUploads",
        "s3:listBucketVersions",
        "s3:listJobs",
        "s3:listMultiRegionAccessPoints",
        "s3:listMultipartUploadParts",
        "s3:listStorageLensConfigurations",
        "s3express:getBucketPolicy",
        "s3express:listAllMyDirectoryBuckets",
        "sagemaker:describeAction",
        "sagemaker:describeAlgorithm",
        "sagemaker:describeApp",
        "sagemaker:describeAppImageConfig",
        "sagemaker:describeArtifact",
        "sagemaker:describeAutoMLJob",
        "sagemaker:describeCluster",
        "sagemaker:describeClusterNode",
        "sagemaker:describeCodeRepository",
        "sagemaker:describeCompilationJob",
        "sagemaker:describeContext",
        "sagemaker:describeDataQualityJobDefinition",
        "sagemaker:describeDevice",
        "sagemaker:describeDeviceFleet",
        "sagemaker:describeDomain",
        "sagemaker:describeEdgeDeploymentPlan",
        "sagemaker:describeEdgePackagingJob",
```

```
        "sagemaker:describeEndpoint",
        "sagemaker:describeEndpointConfig",
        "sagemaker:describeExperiment",
        "sagemaker:describeFeatureGroup",
        "sagemaker:describeFeatureMetadata",
        "sagemaker:describeFlowDefinition",
        "sagemaker:describeHub",
        "sagemaker:describeHubContent",
        "sagemaker:describeHumanTaskUi",
        "sagemaker:describeHyperParameterTuningJob",
        "sagemaker:describeImage",
        "sagemaker:describeImageVersion",
        "sagemaker:describeInferenceComponent",
        "sagemaker:describeInferenceExperiment",
        "sagemaker:describeInferenceRecommendationsJob",
        "sagemaker:describeLabelingJob",
        "sagemaker:describeModel",
        "sagemaker:describeModelBiasJobDefinition",
        "sagemaker:describeModelCard",
        "sagemaker:describeModelCardExportJob",
        "sagemaker:describeModelExplainabilityJobDefinition",
        "sagemaker:describeModelPackage",
        "sagemaker:describeModelPackageGroup",
        "sagemaker:describeModelQualityJobDefinition",
        "sagemaker:describeMonitoringSchedule",
        "sagemaker:describeNotebookInstance",
        "sagemaker:describeNotebookInstanceLifecycleConfig",
        "sagemaker:describePipeline",
        "sagemaker:describePipelineDefinitionForExecution",
        "sagemaker:describePipelineExecution",
        "sagemaker:describeProcessingJob",
        "sagemaker:describeProject",
        "sagemaker:describeSpace",
        "sagemaker:describeStudioLifecycleConfig",
        "sagemaker:describeSubscribedWorkteam",
        "sagemaker:describeTrainingJob",
        "sagemaker:describeTransformJob",
        "sagemaker:describeTrial",
        "sagemaker:describeTrialComponent",
        "sagemaker:describeUserProfile",
        "sagemaker:describeWorkforce",
        "sagemaker:describeWorkteam",
        "sagemaker:getDeviceFleetReport",
        "sagemaker:getModelPackageGroupPolicy",
```

```
        "sagemaker:getSagemakerServicecatalogPortfolioStatus",
        "sagemaker:listActions",
        "sagemaker:listAlgorithms",
        "sagemaker:listAliases",
        "sagemaker:listAppImageConfigs",
        "sagemaker:listApps",
        "sagemaker:listArtifacts",
        "sagemaker:listAssociations",
        "sagemaker:listAutoMLJobs",
        "sagemaker:listCandidatesForAutoMLJob",
        "sagemaker:listClusterNodes",
        "sagemaker:listClusters",
        "sagemaker:listCodeRepositories",
        "sagemaker:listCompilationJobs",
        "sagemaker:listContexts",
        "sagemaker:listDataQualityJobDefinitions",
        "sagemaker:listDeviceFleets",
        "sagemaker:listDevices",
        "sagemaker:listDomains",
        "sagemaker:listEdgeDeploymentPlans",
        "sagemaker:listEdgePackagingJobs",
        "sagemaker:listEndpointConfigs",
        "sagemaker:listEndpoints",
        "sagemaker:listExperiments",
        "sagemaker:listFeatureGroups",
        "sagemaker:listFlowDefinitions",
        "sagemaker:listHubContentVersions",
        "sagemaker:listHubContents",
        "sagemaker:listHubs",
        "sagemaker:listHumanTaskUis",
        "sagemaker:listHyperParameterTuningJobs",
        "sagemaker:listImageVersions",
        "sagemaker:listImages",
        "sagemaker:listInferenceComponents",
        "sagemaker:listInferenceExperiments",
        "sagemaker:listInferenceRecommendationsJobSteps",
        "sagemaker:listInferenceRecommendationsJobs",
        "sagemaker:listLabelingJobs",
        "sagemaker:listLabelingJobsForWorkteam",
        "sagemaker:listLineageGroups",
        "sagemaker:listModelBiasJobDefinitions",
        "sagemaker:listModelCardExportJobs",
        "sagemaker:listModelCardVersions",
        "sagemaker:listModelCards",
```

```
        "sagemaker:listModelExplainabilityJobDefinitions",
        "sagemaker:listModelMetadata",
        "sagemaker:listModelPackageGroups",
        "sagemaker:listModelPackages",
        "sagemaker:listModelQualityJobDefinitions",
        "sagemaker:listModels",
        "sagemaker:listMonitoringAlertHistory",
        "sagemaker:listMonitoringAlerts",
        "sagemaker:listMonitoringExecutions",
        "sagemaker:listMonitoringSchedules",
        "sagemaker:listNotebookInstanceLifecycleConfigs",
        "sagemaker:listNotebookInstances",
        "sagemaker:listPipelineExecutionSteps",
        "sagemaker:listPipelineExecutions",
        "sagemaker:listPipelineParametersForExecution",
        "sagemaker:listPipelines",
        "sagemaker:listProcessingJobs",
        "sagemaker:listProjects",
        "sagemaker:listSpaces",
        "sagemaker:listStageDevices",
        "sagemaker:listStudioLifecycleConfigs",
        "sagemaker:listSubscribedWorkteams",
        "sagemaker:listTags",
        "sagemaker:listTrainingJobs",
        "sagemaker:listTrainingJobsForHyperParameterTuningJob",
        "sagemaker:listTransformJobs",
        "sagemaker:listTrialComponents",
        "sagemaker:listTrials",
        "sagemaker:listUserProfiles",
        "sagemaker:listWorkforces",
        "sagemaker:listWorkteams",
        "scheduler:listScheduleGroups",
        "scheduler:listSchedules",
        "servicequotas:listAWSDefaultServiceQuotas",
        "servicequotas:listServiceQuotas",
        "ses:describeActiveReceiptRuleSet",
        "ses:describeConfigurationSet",
        "ses:describeReceiptRule",
        "ses:describeReceiptRuleSet",
        "ses:getAccount",
        "ses:getAccountSendingEnabled",
        "ses:getBlacklistReports",
        "ses:getConfigurationSet",
        "ses:getConfigurationSetEventDestinations",
```

```
        "ses:getContactList",
        "ses:getDedicatedIp",
        "ses:getDedicatedIpPool",
        "ses:getDedicatedIps",
        "ses:getDeliverabilityDashboardOptions",
        "ses:getDeliverabilityTestReport",
        "ses:getDomainDeliverabilityCampaign",
        "ses:getDomainStatisticsReport",
        "ses:getEmailIdentity",
        "ses:getIdentityDkimAttributes",
        "ses:getIdentityMailFromDomainAttributes",
        "ses:getIdentityNotificationAttributes",
        "ses:getIdentityPolicies",
        "ses:getIdentityVerificationAttributes",
        "ses:getImportJob",
        "ses:getSendQuota",
        "ses:getSendStatistics",
        "ses:listConfigurationSets",
        "ses:listContactLists",
        "ses:listContacts",
        "ses:listCustomVerificationEmailTemplates",
        "ses:listDedicatedIpPools",
        "ses:listDeliverabilityTestReports",
        "ses:listDomainDeliverabilityCampaigns",
        "ses:listEmailIdentities",
        "ses:listEmailTemplates",
        "ses:listIdentities",
        "ses:listIdentityPolicies",
        "ses:listImportJobs",
        "ses:listReceiptFilters",
        "ses:listReceiptRuleSets",
        "ses:listRecommendations",
        "ses:listTagsForResource",
        "ses:listTemplates",
        "ses:listVerifiedEmailAddresses",
        "sns:checkIfPhoneNumberIsOptedOut",
        "sns:getDataProtectionPolicy",
        "sns:getEndpointAttributes",
        "sns:getPlatformApplicationAttributes",
        "sns:getSMSAttributes",
        "sns:getSMSSandboxAccountStatus",
        "sns:getSubscriptionAttributes",
        "sns:getTopicAttributes",
        "sns:listEndpointsByPlatformApplication",
```

```
        "sns:listOriginationNumbers",
        "sns:listPhoneNumbersOptedOut",
        "sns:listPlatformApplications",
        "sns:listSMSSandboxPhoneNumbers",
        "sns:listSubscriptions",
        "sns:listSubscriptionsByTopic",
        "sns:listTopics",
        "ssm-contacts:describeEngagement",
        "ssm-contacts:describePage",
        "ssm-contacts:getContact",
        "ssm-contacts:getContactChannel",
        "ssm-contacts:getContactPolicy",
        "ssm-contacts:getRotation",
        "ssm-contacts:getRotationOverride",
        "ssm-contacts:listContactChannels",
        "ssm-contacts:listContacts",
        "ssm-contacts:listEngagements",
        "ssm-contacts:listPageReceipts",
        "ssm-contacts:listPageResolutions",
        "ssm-contacts:listPagesByContact",
        "ssm-contacts:listPagesByEngagement",
        "ssm-contacts:listPreviewRotationShifts",
        "ssm-contacts:listRotationOverrides",
        "ssm-contacts:listRotationShifts",
        "ssm-contacts:listRotations",
        "ssm-incidents:getIncidentRecord",
        "ssm-incidents:getReplicationSet",
        "ssm-incidents:getResourcePolicies",
        "ssm-incidents:getResponsePlan",
        "ssm-incidents:getTimelineEvent",
        "ssm-incidents:listIncidentRecords",
        "ssm-incidents:listRelatedItems",
        "ssm-incidents:listReplicationSets",
        "ssm-incidents:listResponsePlans",
        "ssm-incidents:listTimelineEvents",
        "ssm-sap:getApplication",
        "ssm-sap:getComponent",
        "ssm-sap:getDatabase",
        "ssm-sap:getOperation",
        "ssm-sap:getResourcePermission",
        "ssm-sap:listApplications",
        "ssm-sap:listComponents",
        "ssm-sap:listDatabases",
        "ssm-sap:listOperations",
```

```
            "ssm:describeActivations",
            "ssm:describeAssociation",
            "ssm:describeAssociationExecutionTargets",
            "ssm:describeAssociationExecutions",
            "ssm:describeAutomationExecutions",
            "ssm:describeAutomationStepExecutions",
            "ssm:describeAvailablePatches",
            "ssm:describeDocument",
            "ssm:describeDocumentPermission",
            "ssm:describeEffectiveInstanceAssociations",
            "ssm:describeEffectivePatchesForPatchBaseline",
            "ssm:describeInstanceAssociationsStatus",
            "ssm:describeInstanceInformation",
            "ssm:describeInstancePatchStates",
            "ssm:describeInstancePatchStatesForPatchGroup",
            "ssm:describeInstancePatches",
            "ssm:describeInventoryDeletions",
            "ssm:describeMaintenanceWindowExecutionTaskInvocations",
            "ssm:describeMaintenanceWindowExecutionTasks",
            "ssm:describeMaintenanceWindowExecutions",
            "ssm:describeMaintenanceWindowSchedule",
            "ssm:describeMaintenanceWindowTargets",
            "ssm:describeMaintenanceWindowTasks",
            "ssm:describeMaintenanceWindows",
            "ssm:describeMaintenanceWindowsForTarget",
            "ssm:describeOpsItems",
            "ssm:describeParameters",
            "ssm:describePatchBaselines",
            "ssm:describePatchGroupState",
            "ssm:describePatchGroups",
            "ssm:describePatchProperties",
            "ssm:describeSessions",
            "ssm:getAutomationExecution",
            "ssm:getCalendarState",
            "ssm:getCommandInvocation",
            "ssm:getConnectionStatus",
            "ssm:getDefaultPatchBaseline",
            "ssm:getDeployablePatchSnapshotForInstance",
            "ssm:getInventorySchema",
            "ssm:getMaintenanceWindow",
            "ssm:getMaintenanceWindowExecution",
            "ssm:getMaintenanceWindowExecutionTask",
            "ssm:getMaintenanceWindowExecutionTaskInvocation",
            "ssm:getMaintenanceWindowTask",
```

```
        "ssm:getOpsItem",
        "ssm:getOpsMetadata",
        "ssm:getOpsSummary",
        "ssm:getPatchBaseline",
        "ssm:getPatchBaselineForPatchGroup",
        "ssm:getResourcePolicies",
        "ssm:getServiceSetting",
        "ssm:listAssociationVersions",
        "ssm:listAssociations",
        "ssm:listCommandInvocations",
        "ssm:listCommands",
        "ssm:listComplianceItems",
        "ssm:listComplianceSummaries",
        "ssm:listDocumentMetadataHistory",
        "ssm:listDocumentVersions",
        "ssm:listDocuments",
        "ssm:listOpsItemEvents",
        "ssm:listOpsItemRelatedItems",
        "ssm:listOpsMetadata",
        "ssm:listResourceComplianceSummaries",
        "ssm:listResourceDataSync",
        "ssm:listTagsForResource",
        "swf:describeActivityType",
        "swf:describeDomain",
        "swf:describeWorkflowExecution",
        "swf:describeWorkflowType",
        "swf:getWorkflowExecutionHistory",
        "swf:listActivityTypes",
        "swf:listClosedWorkflowExecutions",
        "swf:listDomains",
        "swf:listOpenWorkflowExecutions",
        "swf:listWorkflowTypes",
        "vpc-lattice:getAccessLogSubscription",
        "vpc-lattice:getAuthPolicy",
        "vpc-lattice:getListener",
        "vpc-lattice:getResourcePolicy",
        "vpc-lattice:getRule",
        "vpc-lattice:getService",
        "vpc-lattice:getServiceNetwork",
        "vpc-lattice:getServiceNetworkServiceAssociation",
        "vpc-lattice:getServiceNetworkVpcAssociation",
        "vpc-lattice:getTargetGroup",
        "vpc-lattice:listAccessLogSubscriptions",
        "vpc-lattice:listListeners",
```

```
        "vpc-lattice:listRules",
        "vpc-lattice:listServiceNetworkServiceAssociations",
        "vpc-lattice:listServiceNetworkVpcAssociations",
        "vpc-lattice:listServiceNetworks",
        "vpc-lattice:listServices",
        "vpc-lattice:listTargetGroups",
        "vpc-lattice:listTargets",
        "waf-regional:getByteMatchSet",
        "waf-regional:getChangeTokenStatus",
        "waf-regional:getGeoMatchSet",
        "waf-regional:getIPSet",
        "waf-regional:getLoggingConfiguration",
        "waf-regional:getRateBasedRule",
        "waf-regional:getRegexMatchSet",
        "waf-regional:getRegexPatternSet",
        "waf-regional:getRule",
        "waf-regional:getRuleGroup",
        "waf-regional:getSqlInjectionMatchSet",
        "waf-regional:getWebACL",
        "waf-regional:getWebACLForResource",
        "waf-regional:listActivatedRulesInRuleGroup",
        "waf-regional:listByteMatchSets",
        "waf-regional:listGeoMatchSets",
        "waf-regional:listIPSets",
        "waf-regional:listLoggingConfigurations",
        "waf-regional:listRateBasedRules",
        "waf-regional:listRegexMatchSets",
        "waf-regional:listRegexPatternSets",
        "waf-regional:listResourcesForWebACL",
        "waf-regional:listRuleGroups",
        "waf-regional:listRules",
        "waf-regional:listSqlInjectionMatchSets",
        "waf-regional:listWebACLs",
        "waf:getByteMatchSet",
        "waf:getChangeTokenStatus",
        "waf:getGeoMatchSet",
        "waf:getIPSet",
        "waf:getLoggingConfiguration",
        "waf:getRateBasedRule",
        "waf:getRegexMatchSet",
        "waf:getRegexPatternSet",
        "waf:getRule",
        "waf:getRuleGroup",
        "waf:getSampledRequests",
```

```
        "waf:getSizeConstraintSet",
        "waf:getSqlInjectionMatchSet",
        "waf:getWebACL",
        "waf:getXssMatchSet",
        "waf:listActivatedRulesInRuleGroup",
        "waf:listByteMatchSets",
        "waf:listGeoMatchSets",
        "waf:listIPSets",
        "waf:listLoggingConfigurations",
        "waf:listRateBasedRules",
        "waf:listRegexMatchSets",
        "waf:listRegexPatternSets",
        "waf:listRuleGroups",
        "waf:listRules",
        "waf:listSizeConstraintSets",
        "waf:listSqlInjectionMatchSets",
        "waf:listWebACLs",
        "waf:listXssMatchSets",
        "wafv2:checkCapacity",
        "wafv2:describeManagedRuleGroup",
        "wafv2:getIPSet",
        "wafv2:getLoggingConfiguration",
        "wafv2:getPermissionPolicy",
        "wafv2:getRateBasedStatementManagedKeys",
        "wafv2:getRegexPatternSet",
        "wafv2:getRuleGroup",
        "wafv2:getSampledRequests",
        "wafv2:getWebACL",
        "wafv2:getWebACLForResource",
        "wafv2:listAvailableManagedRuleGroups",
        "wafv2:listIPSets",
        "wafv2:listLoggingConfigurations",
        "wafv2:listRegexPatternSets",
        "wafv2:listResourcesForWebACL",
        "wafv2:listRuleGroups",
        "wafv2:listTagsForResource",
        "wafv2:listWebACLs",
        "workspaces-web:getBrowserSettings",
        "workspaces-web:getIdentityProvider",
        "workspaces-web:getNetworkSettings",
        "workspaces-web:getPortal",
        "workspaces-web:getPortalServiceProviderMetadata",
        "workspaces-web:getTrustStoreCertificate",
        "workspaces-web:getUserSettings",
```

```
        "workspaces-web:listBrowserSettings",
        "workspaces-web:listIdentityProviders",
        "workspaces-web:listNetworkSettings",
        "workspaces-web:listPortals",
        "workspaces-web:listTagsForResource",
        "workspaces-web:listTrustStoreCertificates",
        "workspaces-web:listTrustStores",
        "workspaces-web:listUserSettings",
        "workspaces:describeAccount",
        "workspaces:describeAccountModifications",
        "workspaces:describeApplicationAssociations",
        "workspaces:describeIpGroups",
        "workspaces:describeTags",
        "workspaces:describeWorkspaceAssociations",
        "workspaces:describeWorkspaceBundles",
        "workspaces:describeWorkspaceDirectories",
        "workspaces:describeWorkspaceImages",
        "workspaces:describeWorkspaces",
        "workspaces:describeWorkspacesConnectionStatus"
      ],
      "Resource" : [
        "*"
      ]
    }
  ],
  "Version" : "2012-10-17"
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSPCSComputeNodePolicy

説明: PCS AWS クラスターに接続するためのアクセス許可を PCS AWS コンピューティングノードに付与します。

AWSPCSComputeNodePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSPCSComputeNodePolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 6 月 23 日 18:07 UTC
- 編集日時: 2025 年 6 月 23 日 18:07 UTC
- ARN: arn:aws:iam::aws:policy/AWSPCSComputeNodePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する

- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSPCSServiceRolePolicy

説明: お客様に代わってリソースを管理するアクセス許可を PCS に付与します。

AWSPCSServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2024 年 8 月 27 日 16:01 UTC
- 編集日時: 2025 年 9 月 11 日 18:49 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSPCSServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSPCSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "PermissionsToCreatePCSNetworkInterfacesInSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "PermissionsToManagePCSNetworkInterfaces",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterfacePermission"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSPCSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "PermissionsToDescribePCSResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeLaunchTemplates",
```

```
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeImages",
        "ec2:DescribeImageAttribute",
        "ec2:DescribeCapacityReservations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PermissionsToCreatePCSLaunchTemplates",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSPCSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "PermissionsToManagePCSLaunchTemplates",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions",
        "ec2:CreateLaunchTemplateVersion"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSPCSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "PermissionsToTerminatePCSManagedInstances",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSPCSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "PermissionsToPassRoleToEC2",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/*/AWSPCS*",
        "arn:aws:iam::*:role/AWSPCS*",
        "arn:aws:iam::*:role/aws-pcs/*",
        "arn:aws:iam::*:role/*/aws-pcs/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PermissionsToControlClusterInstanceAttributes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateFleet"
      ],
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:launch-template/*",
```

```
        "arn:aws:ec2:*:*:placement-group/*",
        "arn:aws:ec2:*:*:capacity-reservation/*",
        "arn:aws:resource-groups:*:*:group/*",
        "arn:aws:ec2:*:*:fleet/*",
        "arn:aws:ec2:*:*:spot-instances-request/*"
      ]
    },
    {
      "Sid" : "PermissionsToProvisionClusterInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateFleet"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSPCSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "PermissionsToTagPCSResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances",
            "CreateLaunchTemplate",
            "CreateFleet",
            "CreateNetworkInterface"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "PermissionsToPublishMetrics",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/PCS"
        }
      }
    },
    {
      "Sid" : "PermissionsToManageSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue",
        "secretsmanager:UpdateSecretVersionStage",
        "secretsmanager:DeleteSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:pcs!*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "pcs",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSPriceListServiceFullAccess

説明: AWS Price List Service へのフルアクセスを提供します。

`AWSPriceListServiceFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSPriceListServiceFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 11 月 22 日 00:36 UTC
- 編集日時: 2024 年 7 月 2 日 13:34 UTC
- ARN: arn:aws:iam::aws:policy/AWSPriceListServiceFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する

- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSPrivateCAAuditor

説明: 監査者に Private Certificate Authority AWS へのアクセスを提供します

AWSPrivateCAAuditor は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSPrivateCAAuditor をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 2 月 14 日 18:33 UTC
- 編集日時: 2023 年 2 月 14 日 18:33 UTC
- ARN: arn:aws:iam::aws:policy/AWSPrivateCAAuditor

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSPrivateCAConnectorForKubernetesPolicy

説明: AWS Private CA Connector for Kubernetes に必要なアクセス許可を付与します。

`AWSPrivateCAConnectorForKubernetesPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSPrivateCAConnectorForKubernetesPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 5 月 19 日 19:22 UTC
- 編集日時: 2025 年 5 月 19 日 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateCAConnectorForKubernetesPolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:GetCertificate",
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSPrivateCAFullAccess

説明: AWS プライベート認証機関へのフルアクセスを提供します

AWSPrivateCAFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSPrivateCAFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 2 月 14 日 18:20 UTC
- 編集日時: 2023 年 2 月 14 日 18:20 UTC
- ARN: arn:aws:iam::aws:policy/AWSPrivateCAFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSPrivateCAPrivilegedUser

説明: プライベート認証機関への特権 AWS 証明書ユーザーアクセスを提供します

AWSPrivateCAPrivilegedUser は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSPrivateCAPrivilegedUser をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 2 月 14 日 18:26 UTC
- 編集日時: 2025 年 1 月 22 日 21:07 UTC
- ARN: arn:aws:iam::aws:policy/AWSPrivateCAPrivilegedUser

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "ArnLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:*:*:template/*CACertificate*/V*"
          ]
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "ArnNotLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:*:*:template/*CACertificate*/V*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:RevokeCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:ListPermissions"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:ListCertificateAuthorities"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSPrivateCAReadOnly

説明: AWS プライベート認証機関への読み取り専用アクセスを提供します

AWSPrivateCAReadOnly は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSPrivateCAReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 2 月 14 日 18:30 UTC
- 編集日時: 2023 年 2 月 14 日 18:30 UTC
- ARN: arn:aws:iam::aws:policy/AWSPrivateCAReadOnly

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSPrivateCAUser

説明: 証明書ユーザーに AWS Private Certificate Authority へのアクセスを提供します

AWSPrivateCAUser は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSPrivateCAUser をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 2 月 14 日 18:16 UTC
- 編集日時: 2025 年 1 月 22 日 21:22 UTC
- ARN: arn:aws:iam::aws:policy/AWSPrivateCAUser

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "ArnLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:*:*:template/EndEntityCertificate/V*"
          ]
        }
      }
    },
    {
      "Effect" : "Deny",
```

```
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "ArnNotLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:*:*:template/EndEntityCertificate/V*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:RevokeCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:ListPermissions"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:ListCertificateAuthorities"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSPrivateMarketplaceAdminFullAccess

説明: AWS Private Marketplace のすべての管理アクションへのフルアクセスを提供します。

AWSPrivateMarketplaceAdminFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSPrivateMarketplaceAdminFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 11 月 27 日 16:32 UTC
- 編集日時: 2025 年 6 月 11 日 16:22 UTC
- ARN: arn:aws:iam::aws:policy/AWSPrivateMarketplaceAdminFullAccess

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PrivateMarketplaceGetRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/*AWSServiceRoleForPrivateMarketplaceAdmin"
      ]
    },
    {
      "Sid" : "PrivateMarketplaceCreateSLRPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/private-
marketplace.marketplace.amazonaws.com/AWSServiceRoleForPrivateMarketplaceAdmin"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "private-marketplace.marketplace.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PrivateMarketplaceManageDelegatedAdministratorPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "private-
marketplace.marketplace.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PrivateMarketplaceEnableServiceAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "private-
marketplace.marketplace.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PrivateMarketplaceRequestPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:AssociateProductsWithPrivateMarketplace",
        "aws-marketplace:DisassociateProductsFromPrivateMarketplace",
        "aws-marketplace:ListPrivateMarketplaceRequests",
        "aws-marketplace:DescribePrivateMarketplaceRequests"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "PrivateMarketplaceCatalogAPIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListEntities",
        "aws-marketplace:DescribeEntity",
        "aws-marketplace:StartChangeSet",
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:CancelChangeSet"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PrivateMarketplaceCatalogTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:TagResource",
        "aws-marketplace:UntagResource",
        "aws-marketplace:ListTagsForResource"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/*"
    },
    {
      "Sid" : "PrivateMarketplaceOrganizationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:ListRoots",
        "organizations:ListParents",
        "organizations:ListOrganizationalUnitsForParent",
```

```
        "organizations:ListAccountsForParent",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSPrivateMarketplaceRequests

説明: Private Marketplace AWS でリクエストを作成するアクセスを提供します。

`AWSPrivateMarketplaceRequests` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSPrivateMarketplaceRequests` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 10 月 28 日 21:44 UTC
- 編集日時: 2025 年 11 月 19 日 19:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateMarketplaceRequests`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LegacyPrivateMarketplaceRequestsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:CreatePrivateMarketplaceRequests",
        "aws-marketplace:ListPrivateMarketplaceRequests",
        "aws-marketplace:DescribePrivateMarketplaceRequests"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PrivateMarketplaceManageRequestsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:StartChangeSet"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ProductProcurementRequest/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ChangeSet/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "catalog:ChangeType" : [
            "CreateProductProcurementRequest",
            "CancelProductProcurementRequest"
          ]
        }
      }
    },
    {
      "Sid" : "PrivateMarketplaceReadRequestsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity"
```

```
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ProductProcurementRequest/*"
      ]
    },
    {
      "Sid" : "PrivateMarketplaceListRequestsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListEntities",
        "aws-marketplace:ListChangeSets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PrivateMarketplaceReadChangeSetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeChangeSet"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ChangeSet/*"
      ]
    },
    {
      "Sid" : "PrivateMarketplaceTaggingRequestsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:TagResource",
        "aws-marketplace:UntagResource",
        "aws-marketplace:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ProductProcurementRequest/*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSPrivateNetworksServiceRolePolicy

説明: AWS Private Networks Service がお客様に代わってリソースを管理できるようにします。

AWSPrivateNetworksServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 12 月 16 日 23:17 UTC
- 編集日時: 2021 年 12 月 16 日 23:17 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSPrivateNetworksServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Private5G"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSProtonCodeBuildProvisioningBasicAccess

説明: Permissions CodeBuild は AWS Proton CodeBuild プロビジョニング用のビルドを実行する必要があります。

`AWSProtonCodeBuildProvisioningBasicAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSProtonCodeBuildProvisioningBasicAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 11 月 9 日 21:04 UTC
- 編集日時: 2022 年 11 月 9 日 21:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSProtonCodeBuildProvisioningBasicAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSProtonCodeBuildProvisioningServiceRolePolicy

説明: AWS Proton がユーザーに代わって CodeBuild およびその他の AWS サービスを使用して Proton リソースプロビジョニングを管理できるようにします。

AWSProtonCodeBuildProvisioningServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 11 月 9 日 21:32 UTC
- 編集日時: 2023 年 5 月 17 日 16:11 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSProtonCodeBuildProvisioningServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSProtonDeveloperAccess

説明: AWS Proton APIs とマネジメントコンソールへのアクセスを提供しますが、Proton テンプレートまたは環境の管理は許可しません。

`AWSProtonDeveloperAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSProtonDeveloperAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 2 月 17 日 19:02 UTC
- 編集日時: 2024 年 6 月 6 日 18:26 UTC
- ARN: `arn:aws:iam::aws:policy/AWSProtonDeveloperAccess`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSProtonFullAccess

説明: AWS Proton APIs とマネジメントコンソールへのフルアクセスを提供します。これらの許可に加えて、S3 バケットからテンプレートバンドルを登録するには Amazon S3 へのアクセスも必要です。また、Proton のサービスロールを作成および管理するための Amazon IAM へのアクセスも必要です。

`AWSProtonFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSProtonFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 2 月 17 日 19:07 UTC
- 編集日時: 2024 年 6 月 6 日 18:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSProtonFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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"
```

```
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSProtonReadOnlyAccess

説明: AWS Proton APIs とマネジメントコンソールへの読み取り専用アクセスを提供します。

`AWSProtonReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSProtonReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 2 月 17 日 19:09 UTC
- 編集日時: 2022 年 11 月 18 日 18:28 UTC
- ARN: `arn:aws:iam::aws:policy/AWSProtonReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSProtonServiceGitSyncServiceRolePolicy

説明: AWS Proton がサービス、環境、コンポーネント定義を git リポジトリから AWS Proton に同期できるようにするポリシー。

AWSProtonServiceGitSyncServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー

- 作成日時: 2023 年 4 月 4 日 15:55 UTC
- 編集日時: 2023 年 4 月 4 日 15:55 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSProtonServiceGitSyncServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSProtonSyncServiceRolePolicy

説明: AWS Proton が git リポジトリのコンテンツを Proton に同期するか、Proton のコンテンツを git リポジトリに同期することを許可するポリシー。

AWSProtonSyncServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 11 月 23 日 21:14 UTC
- 編集日時: 2024 年 5 月 5 日 01:49 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSProtonSyncServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSPurchaseOrdersServiceRolePolicy

説明: 請求コンソールで注文書を表示および変更する許可を付与

AWSPurchaseOrdersServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSPurchaseOrdersServiceRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 5 月 6 日 18:15 UTC
- 編集日時: 2024 年 12 月 1 日 17:51 UTC
- ARN: arn:aws:iam::aws:policy/AWSPurchaseOrdersServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
        "account:GetContactInformation",
        "aws-portal:*Billing",
        "consolidatedbilling:GetAccountBillingRole",
        "invoicing:GetInvoicePDF",
        "invoicing:ListInvoiceUnits",
        "payments:GetPaymentInstrument",
        "payments:ListPaymentPreferences",
        "purchase-orders:AddPurchaseOrder",
        "purchase-orders:DeletePurchaseOrder",
        "purchase-orders:GetPurchaseOrder",
        "purchase-orders:ListPurchaseOrderInvoices",
        "purchase-orders:ListPurchaseOrders",
        "purchase-orders:ListTagsForResource",
        "purchase-orders:ModifyPurchaseOrders",
        "purchase-orders:TagResource",
        "purchase-orders:UntagResource",
        "purchase-orders:UpdatePurchaseOrder",
        "purchase-orders:UpdatePurchaseOrderStatus",
        "purchase-orders:ViewPurchaseOrders",
        "tax:ListTaxRegistrations"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSQuickSetupCFGCPacksPermissionsBoundary

説明: AWSQuickSetupCFGCPacksPermissionsBoundary ポリシーは、Quick Setup によって作成された IAM ロールに対して付与されるアクセス許可のリストを定義します。高速セットアップでは、このポリシーで作成されたロールを使用して AWS Config コンフォーマンスパックをデプロイします。

AWSQuickSetupCFGCPacksPermissionsBoundary は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSQuickSetupCFGCPacksPermissionsBoundary をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 6 月 26 日 09:52 UTC
- 編集日時: 2024 年 6 月 26 日 09:52 UTC
- ARN: arn:aws:iam::aws:policy/AWSQuickSetupCFGCPacksPermissionsBoundary

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-CFGCPacks*"
      ]
    },
    {
      "Sid" : "ConfigurationRolePassToSSMPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-CFGCPacks*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PutCPackPermissions",
      "Effect" : "Allow",
      "Action" : [
        "config:PutConformancePack"
      ],
      "Resource" : [
        "arn:aws:config:*:*:conformance-pack/AWS-QuickSetup-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : [
            "${aws:PrincipalAccount}"
          ]
        }
      }
    },
    {
      "Sid" : "DescribeCPacksPermissions",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConformancePackStatus"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConformancePacksSLRCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/config-conforms.amazonaws.com/
AWSServiceRoleForConfigConforms"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "config-conforms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SystemsManagerSLRCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EnableExplorerReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "config:DescribeConfigurationRecorders",
        "compute-optimizer:GetEnrollmentStatus",
        "support:DescribeTrustedAdvisorChecks"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "ServiceSettingsForExplorerUpdatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/ssm-patchmanager",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/EC2",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ExplorerOnboarded",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/Association",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ComputeOptimizer",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ConfigCompliance",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/OpsData-TrustedAdvisor",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/SupportCenterCase"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSQuickSetupDeploymentRolePolicy

説明: 複数の設定タイプをデプロイするための AWS Systems Manager 高速セットアップのアクセス許可を提供します。これらの設定タイプは、推奨されるベストプラクティスを使用して、頻繁に使用される Amazon Web Services のサービスと機能を設定する IAM ロールとオートメーションを作成します。

AWSQuickSetupDeploymentRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSQuickSetupDeploymentRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 6 月 26 日 09:55 UTC
- 編集日時: 2025 年 12 月 17 日 15:49 UTC
- ARN: arn:aws:iam::aws:policy/AWSQuickSetupDeploymentRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CfnRead",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackDriftDetectionStatus",
        "cloudformation:ListStacks"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CfnManage",
      "Effect" : "Allow",
```

```
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack",
        "cloudformation:DeleteStack",
        "cloudformation:CreateChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackResourceDrifts",
        "cloudformation:DetectStackDrift",
        "cloudformation:DetectStackResourceDrift"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/StackSet-AWS-QuickSetup-*"
      ]
    },
    {
      "Sid" : "RGroupsGet",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:GetGroupQuery"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CPacksRead",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConformancePacks",
        "config:DescribeConformancePackStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OpsPacksManage",
      "Effect" : "Allow",
      "Action" : [
        "config:PutConformancePack",
        "config:DeleteConformancePack"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
```

```
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : "arn:aws:config:*:*:conformance-pack/AWS-QuickSetup-*"
    },
    {
      "Sid" : "QSDocsManage",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateDocument",
        "ssm:UpdateDocument",
        "ssm:UpdateDocumentDefaultVersion",
        "ssm:DeleteDocument",
        "ssm:AddTagsToResource",
        "ssm:RemoveTagsFromResource",
        "ssm:ListTagsForResource"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSQuickSetup-*",
        "arn:aws:ssm:*:*:document/AWSOperationsPack-*",
        "arn:aws:ssm:*:*:document/AWSOperationsPackInstance-*"
      ]
    },
    {
      "Sid" : "QSDocsRead",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSQuickSetup-*",
        "arn:aws:ssm:*:*:document/AWSOperationsPack*",
        "arn:aws:ssm:*::document/AWSConformancePacks-*",
        "arn:aws:ssm:*::document/AWSEC2-UpdateLaunchAgent",
        "arn:aws:ssm:*::document/AWS-ConfigureAWSPackage",
```

```
        "arn:aws:ssm:*::document/AWS-EnableExplorer",
        "arn:aws:ssm:*::document/AWS-GatherSoftwareInventory",
        "arn:aws:ssm:*::document/AWS-RunPatchBaselineAssociation",
        "arn:aws:ssm:*::document/AWS-UpdateSSMAgent",
        "arn:aws:ssm:*::document/AWSQuickSetupType-ManageInstanceProfile",
        "arn:aws:ssm:*::document/AWSQuickSetupType-EnableConfigRecording",
        "arn:aws:ssm:*::document/AWSQuickSetupType-Scheduler-ChangeCalendarState",
        "arn:aws:ssm:*::document/AmazonCloudWatch-ManageAgent",
        "arn:aws:ssm:*::document/AWSQuickSetupType-InstallAndManageCloudWatchAgent",
        "arn:aws:ssm:*::document/AWSQuickSetupType-ConfigureDevOpsGuru",
        "arn:aws:ssm:*::document/AWSQuickSetupType-DeployConformancePack",
        "arn:aws:ssm:*::document/AWSQuickSetupType-Scheduler-ApplyInstanceState"
      ]
    },
    {
      "Sid" : "QSAssociationsManage",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:UpdateAssociation",
        "ssm:DeleteAssociation",
        "ssm:DescribeAssociation"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSQuickSetup-*",
        "arn:aws:ssm:*:*:document/AWSOperationsPack*",
        "arn:aws:ssm:*::document/AWSEC2-UpdateLaunchAgent",
        "arn:aws:ssm:*::document/AWS-ConfigureAWSPackage",
        "arn:aws:ssm:*::document/AWS-EnableExplorer",
        "arn:aws:ssm:*::document/AWS-GatherSoftwareInventory",
        "arn:aws:ssm:*::document/AWS-RunPatchBaselineAssociation",
        "arn:aws:ssm:*::document/AWS-UpdateSSMAgent",
        "arn:aws:ssm:*::document/AWSQuickSetupType-ManageInstanceProfile",
        "arn:aws:ssm:*::document/AWSQuickSetupType-EnableConfigRecording",
        "arn:aws:ssm:*::document/AWSQuickSetupType-Scheduler-ChangeCalendarState",
        "arn:aws:ssm:*::document/AWSQuickSetupType-Scheduler-ApplyInstanceState",
        "arn:aws:ssm:*::document/AmazonCloudWatch-ManageAgent",
```

```
        "arn:aws:ssm:*::document/AWSQuickSetupType-InstallAndManageCloudWatchAgent",
        "arn:aws:ssm:*::document/AWSQuickSetupType-ConfigureDevOpsGuru",
        "arn:aws:ssm:*::document/AWSQuickSetupType-DeployConformancePack",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*:*:association/*"
      ]
    },
    {
      "Sid" : "EventRulesManage",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:PutRule",
        "events:DeleteRule",
        "events:ListTargetsByRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/*QuickSetup-*"
      ]
    },
    {
      "Sid" : "CPacksSLRCreate",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/config-conforms.amazonaws.com/
AWSServiceRoleForConfigConforms"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "config-conforms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SSMSLRCreate",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
```

```
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "QSConfigRoleManage",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:GetRole",
        "iam:UpdateRole",
        "iam:DeleteRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:ListRoleTags",
        "iam:TagRole",
        "iam:UntagRole"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-*",
        "arn:aws:iam::*:role/AWSOperationsPack-*"
      ]
    },
    {
      "Sid" : "QSConfigRolePass",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
```

```
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-*",
        "arn:aws:iam::*:role/AWSOperationsPack-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com",
            "events.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DocDescribe",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "LegacyDocClean",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteDocument"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/QuickSetupID" : "*"
        }
      }
    },
    {
      "Sid" : "LegacyIAMClean",
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:DeleteRole",
        "iam:DeleteRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/*QuickSetup-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/QuickSetupID" : "*"
        }
      }
    },
    {
      "Sid" : "QSConfigRoleBounded",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRolePolicy",
        "iam:PutRolePolicy",
        "iam:PutRolePermissionsBoundary"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PermissionsBoundary" : [
            "arn:aws:iam::aws:policy/AWSQuickSetupCFGCPacksPermissionsBoundary",
            "arn:aws:iam::aws:policy/AWSQuickSetupCFGRecordingPermissionsBoundary",
            "arn:aws:iam::aws:policy/AWSQuickSetupDevOpsGuruPermissionsBoundary",
            "arn:aws:iam::aws:policy/AWSQuickSetupDistributorPermissionsBoundary",
            "arn:aws:iam::aws:policy/AWSQuickSetupSchedulerPermissionsBoundary",
            "arn:aws:iam::aws:policy/AWSQuickSetupSSMHostMgmtPermissionsBoundary"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-*",
        "arn:aws:iam::*:role/AWSOperationsPack-*"
      ]
    },
    {
      "Sid" : "QSConfigRoleManagedPolicies",
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/AWSSystemsManagerEnableExplorerExecutionPolicy",
            "arn:aws:iam::aws:policy/
AWSSystemsManagerEnableConfigRecordingExecutionPolicy",
            "arn:aws:iam::aws:policy/
AWSQuickSetupManagedInstanceProfileExecutionPolicy",
            "arn:aws:iam::aws:policy/AWSQuickSetupStartStopInstancesExecutionPolicy",
            "arn:aws:iam::aws:policy/AWSQuickSetupStartSSMAssociationsExecutionPolicy"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-*",
        "arn:aws:iam::*:role/AWSOperationsPack-*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSQuickSetupDevOpsGuruPermissionsBoundary

説明 : AWSQuickSetupDevOpsGuruPermissionsBoundary ポリシーは、Quick Setup によって作成された IAM ロールに付与されるアクセス許可のリストを定義します。Quick Setup は、このポリシーで作成されたロールを使用して Amazon DevOps Guru を有効にして設定します。このポリシーは、Systems Manager Explorer を有効にするアクセス許可も提供します。

AWSQuickSetupDevOpsGuruPermissionsBoundary は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSQuickSetupDevOpsGuruPermissionsBoundary をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 6 月 26 日 09:44 UTC
- 編集日時: 2024 年 6 月 26 日 09:44 UTC
- ARN: arn:aws:iam::aws:policy/AWSQuickSetupDevOpsGuruPermissionsBoundary

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CreateDevOpsGuruSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/devops-guru.amazonaws.com/
AWSServiceRoleForDevOpsGuru"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "devops-guru.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudformationReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStacks",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DevOpsGuruNotificationChannelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "devops-guru:AddNotificationChannel"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:DevOpsGuru-Default-Topic",
```

```
        "arn:aws:devops-guru:*:*:/channels"
      ]
    },
    {
      "Sid" : "DevOpsGuruConfigurationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "devops-guru:UpdateResourceCollection",
        "devops-guru:UpdateServiceIntegration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SNSReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DevOpsGuruDefaultSNSTopicConfigurationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sns:AddPermission",
        "sns:CreateTopic",
        "sns:GetTopicAttributes",
        "sns:Publish",
        "sns:SetTopicAttributes",
        "sns:RemovePermission"
      ],
      "Resource" : "arn:aws:sns:*:*:DevOpsGuru-Default-Topic"
    },
    {
      "Sid" : "ReadOnlyPermissionsForEnablingExplorer",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "config:DescribeConfigurationRecorders",
        "compute-optimizer:GetEnrollmentStatus",
        "support:DescribeTrustedAdvisorChecks"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "SSMExplorerServiceSettingsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/ssm-patchmanager",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/EC2",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ExplorerOnboarded",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/Association",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ComputeOptimizer",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ConfigCompliance",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/OpsData-TrustedAdvisor",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/SupportCenterCase"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSQuickSetupDistributorPermissionsBoundary

説明: QuickSetup は、ユーザーに代わって Systems Manager Distributor 機能を設定できるようにする IAM ロールを作成しますが、そのようなロール作成時にこのポリシーを使用してアクセス許可の範囲を定義します。

`AWSQuickSetupDistributorPermissionsBoundary` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSQuickSetupDistributorPermissionsBoundary` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 6 月 26 日 09:50 UTC
- 編集日時: 2024 年 6 月 26 日 09:50 UTC
- ARN: arn:aws:iam::aws:policy/AWSQuickSetupDistributorPermissionsBoundary

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DistributorAutomationRoleGetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-RoleForDistributor-*"
      ]
    },
    {
      "Sid" : "DistributorAutomationRolePassPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-RoleForDistributor-*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DefaultInstanceRoleManagePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:UpdateRole",
        "iam:GetRole"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:PrincipalTag/QuickSetupManagerID" : "*"
        },
        "ArnLike" : {
          "aws:PrincipalArn" : "arn:aws:iam::*:role/AWS-QuickSetup-RoleForDistributor-
*"
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup"
      ]
    },
    {
      "Sid" : "DefaultInstanceRolePassToEC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "DefaultInstanceRolePassToSSMPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "InstanceManagementPoliciesAttachPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/AmazonElasticFileSystemsUtils",
            "arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore"
          ]
        },
        "StringLike" : {
          "aws:PrincipalTag/QuickSetupManagerID" : "*"
        },
        "ArnLike" : {
          "aws:PrincipalArn" : "arn:aws:iam::*:role/AWS-QuickSetup-RoleForDistributor-
*"
        }
      },
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
```

```
      "Sid" : "CreateSystemsManagerSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DefaultInstanceRoleAddPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:AddRoleToInstanceProfile"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "IAMReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile",
        "iam:GetRolePolicy",
        "iam:ListInstanceProfilesForRole",
        "iam:ListRoles"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DefaultInstanceProfileCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateInstanceProfile"
      ],
```

```
      "Resource" : [
        "arn:aws:iam::*:instance-profile/AmazonSSMRoleForInstancesQuickSetup"
      ]
    },
    {
      "Sid" : "DefaultInstanceProfileAssociationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateIamInstanceProfile"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "ec2:InstanceProfile" : "true"
        },
        "ArnLike" : {
          "ec2:NewInstanceProfile" : "arn:aws:iam::*:instance-profile/
AmazonSSMRoleForInstancesQuickSetup"
        }
      }
    },
    {
      "Sid" : "DefaultInstanceProfileDisassociationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DisassociateIamInstanceProfile"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ec2:InstanceProfile" : "arn:aws:iam::*:instance-profile/
AmazonSSMRoleForInstancesQuickSetup"
        }
      }
    },
    {
      "Sid" : "ConfigurationAutomationsStartPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-definition/AWSQuickSetup-Distributor-*",
        "arn:aws:ssm:*:*:automation-definition/UpdateCloudWatchDocument-Distributor-*",
```

```
        "arn:aws:ssm:*:*:automation-definition/AWS-ConfigureAWSPackage*",
        "arn:aws:ssm:*:*:automation-definition/AWS-AttachIAMToInstance*"
      ]
    },
    {
      "Sid" : "ReadOnlyPermissionsForEnablingHostManagementBySSM",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListTagsForResource",
        "ssm:GetAutomationExecution",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ReadOnlyPermissionsForEnablingExplorer",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigurationRecorders",
        "compute-optimizer:GetEnrollmentStatus",
        "support:DescribeTrustedAdvisorChecks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMExplorerServiceSettingsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/ssm-patchmanager",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/EC2",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ExplorerOnboarded",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/Association",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ComputeOptimizer",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ConfigCompliance",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/OpsData-TrustedAdvisor",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/SupportCenterCase"
      ]
    }
  ]
```

```
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSQuickSetupEnableAREXExecutionPolicy

説明: このポリシーは、Systems Manager が AWSQuickSetupType-EnableAREX Automation ランブックを実行できるようにするアクセス許可を付与します。これにより、 AWS Resource Explorer は Systems Manager で使用できます。

`AWSQuickSetupEnableAREXExecutionPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSQuickSetupEnableAREXExecutionPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 11 月 15 日 22:45 UTC
- 編集日時: 2024 年 11 月 15 日 22:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupEnableAREXExecutionPolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadActions",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:GetDefaultView",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListViews"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowUpdateExistingIndexAndAssociateDefaultView",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:UpdateIndexType",
        "resource-explorer-2:AssociateDefaultView"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCreateViewAndIndex",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:CreateView",
        "resource-explorer-2:CreateIndex",
        "resource-explorer-2:TagResource"
      ],
      "Resource" : [
        "arn:aws:resource-explorer-2:*:*:view/all-resources/*",
        "arn:aws:resource-explorer-2:*:*:index/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/Type" : "QuickSetup",
          "aws:ResourceTag/Type" : "QuickSetup"
        },
        "ForAllValues:StringEquals" : {
```

```
          "aws:TagKeys" : "Type"
        }
      }
    },
    {
      "Sid" : "AllowCreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "resource-explorer-2.amazonaws.com"
          ]
        }
      },
      "Resource" : "arn:aws:iam::*:role/aws-service-role/resource-
explorer-2.amazonaws.com/AWSServiceRoleForResourceExplorer"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSQuickSetupEnableDHMCExecutionPolicy

説明: このポリシーは、プリンシパルが AWSQuickSetupType-EnableDHMC Automation ランブックを実行してデフォルトのホスト管理設定を有効にすることを許可するアクセス許可を付与します。

AWSQuickSetupEnableDHMCExecutionPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSQuickSetupEnableDHMCExecutionPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 11 月 15 日 21:27 UTC
- 編集日時: 2024 年 11 月 15 日 21:27 UTC
- ARN: arn:aws:iam::aws:policy/AWSQuickSetupEnableDHMCExecutionPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/AWS-QuickSetup-SSM-DefaultEC2MgmtRole-*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/AWS-QuickSetup-SSM-DefaultEC2MgmtRole-*",
      "Condition" : {
        "StringEquals" : {
```

```
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/AWS-QuickSetup-SSM-DefaultEC2MgmtRole-*",
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : "arn:aws:iam::aws:policy/
AmazonSSMManagedEC2InstanceDefaultPolicy"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetServiceSetting",
        "ssm:UpdateServiceSetting"
      ],
      "Resource" : "arn:aws:ssm:*:*:servicesetting/ssm/managed-instance/default-ec2-
instance-management-role"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSQuickSetupJITNADeploymentRolePolicy

説明: このポリシーにより、Quick Setup はジャストインタイムノードアクセスのセットアップに必要な設定タイプをデプロイできます。

AWSQuickSetupJITNADeploymentRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSQuickSetupJITNADeploymentRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 4 月 17 日 09:07 UTC
- 編集日時: 2025 年 4 月 17 日 09:07 UTC
- ARN: arn:aws:iam::aws:policy/AWSQuickSetupJITNADeploymentRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack",
        "cloudformation:DeleteStack",
        "cloudformation:CreateChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackResourceDrifts",
        "cloudformation:DetectStackDrift",
        "cloudformation:DetectStackResourceDrift",
        "cloudformation:DescribeStackEvents"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/StackSet-AWS-QuickSetup-JITNA-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:UpdateAssociation",
        "ssm:DeleteAssociation",
        "ssm:DescribeAssociation",
        "ssm:GetDocument",
        "ssm:DescribeDocument"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ssm:*::document/AWSQuickSetupType-SetupJITNAResources",
        "arn:aws:ssm:*::document/AWSQuickSetupType-
PropagateJustInTimeNodeAccessPolicies",
        "arn:aws:ssm:*:*:association/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "iam:CreateRole",
        "iam:TagRole"
      ],
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "QuickSetup*"
          ]
        },
        "StringEquals" : {
          "aws:CalledViaLast" : [
            "cloudformation.amazonaws.com"
          ],
          "aws:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-JITNA"
          ],
          "aws:RequestTag/QuickSetupDocument" : [
            "AWSQuickSetupType-JITNA"
          ]
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-EnableJITNA-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:DeleteRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:ListRoleTags"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-EnableJITNA-*"
```

```
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::*:policy/AWSQuickSetupManageJITNAResourcesExecutionPolicy"
          ]
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-EnableJITNA-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-EnableJITNA-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com",
          "iam:ResourceTag/QuickSetupDocument" : "AWSQuickSetupType-JITNA"
        },
        "ArnLike" : {
          "iam:AssociatedResourceARN" : [
            "arn:aws:ssm:*::document/AWSQuickSetupType-SetupJITNAResources",
            "arn:aws:ssm:*:*:association/*"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSQuickSetupManagedInstanceProfileExecutionPolicy

説明: このポリシーは、Quick Setup 機能のデフォルトの IAM インスタンスプロファイルを作成して、まだインスタンスプロファイルがアタッチされていない Amazon EC2 インスタンスにアタッチすることを Systems Manager に許可する管理アクセス許可を付与します。

`AWSQuickSetupManagedInstanceProfileExecutionPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSQuickSetupManagedInstanceProfileExecutionPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 11 月 15 日 21:51 UTC
- 編集日時: 2025 年 11 月 5 日 19:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupManagedInstanceProfileExecutionPolicy`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile",
        "iam:ListInstanceProfilesForRole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DefaultInstanceRoleManagePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup"
    },
    {
      "Sid" : "DefaultInstanceProfileCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/AmazonSSMRoleForInstancesQuickSetup"
      ]
    },
    {
      "Sid" : "DefaultInstanceRoleAddPermissions",
      "Effect" : "Allow",
      "Action" : "iam:AddRoleToInstanceProfile",
      "Resource" : [
        "arn:aws:iam::*:instance-profile/AmazonSSMRoleForInstancesQuickSetup"
      ]
    },
    {
      "Sid" : "DefaultInstanceProfileAssociationPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateIamInstanceProfile"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "ec2:InstanceProfile" : "true"
        },
        "ArnLike" : {
          "ec2:NewInstanceProfile" : "arn:aws:iam::*:instance-profile/
AmazonSSMRoleForInstancesQuickSetup"
        }
      }
    },
    {
      "Sid" : "DefaultInstanceRolePassToEC2Permissions",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "InstanceManagementPoliciesAttachAmazonSSMManagedInstanceCore",
      "Effect" : "Allow",
      "Action" : "iam:AttachRolePolicy",
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore",
            "arn:aws:iam::aws:policy/AmazonSSMPatchAssociation",
            "arn:aws:iam::aws:policy/AWSQuickSetupPatchPolicyBaselineAccess",
            "arn:aws:iam::aws:policy/AmazonElasticFileSystemsUtils",
            "arn:aws:iam::aws:policy/CloudWatchAgentServerPolicy"
          ]
        }
      },
      "Resource" : "arn:aws:iam::*:role/*"
```

```
    },
    {
      "Sid" : "InstanceProfileAssociationEc2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AutomationsStartWithTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution",
        "ssm:AddTagsToResource"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:document/AWS-AttachIAMToInstance*",
        "arn:aws:ssm:*:*:automation-definition/AWS-AttachIAMToInstance*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/InvokedBy" : [
            "AWSQuickSetupType-ManageInstanceProfile"
          ],
          "aws:ResourceTag/InvokedBy" : [
            "AWSQuickSetupType-ManageInstanceProfile"
          ]
        }
      }
    },
    {
      "Sid" : "AutomationsGetPermissions",
      "Effect" : "Allow",
      "Action" : "ssm:GetAutomationExecution",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/InvokedBy" : [
            "AWSQuickSetupType-ManageInstanceProfile"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "GetQuickSetupAutomationAssumeRoles",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM",
            "AWSQuickSetupType-SSMHostMgmt",
            "AWSQuickSetupType-PatchPolicy",
            "AWSQuickSetupType-Distributor",
            "AWSQuickSetupType-CWASetup"
          ]
        }
      }
    },
    {
      "Sid" : "PassQuickSetupAutomationAssumeRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ],
          "iam:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM",
            "AWSQuickSetupType-SSMHostMgmt",
            "AWSQuickSetupType-PatchPolicy",
            "AWSQuickSetupType-Distributor",
            "AWSQuickSetupType-CWASetup"
          ]
        }
      }
```

```
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSQuickSetupManageJITNAResourcesExecutionPolicy

説明: このポリシーは、Systems Manager のジャストインタイムノードアクセスを有効にするアクセス許可を提供します。

`AWSQuickSetupManageJITNAResourcesExecutionPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSQuickSetupManageJITNAResourcesExecutionPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 4 月 17 日 21:37 UTC
- 編集日時: 2025 年 4 月 23 日 15:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupManageJITNAResourcesExecutionPolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateJustInTimeAccessServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/justintimeaccess.ssm.amazonaws.com/
AWSServiceRoleForSystemsManagerJustInTimeAccess"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "justintimeaccess.ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CreateSystemsManagerNotificationServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/notifications.ssm.amazonaws.com/
AWSServiceRoleForSystemsManagerNotifications"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "notifications.ssm.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:AttachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/SSM-JustInTimeAccessTokenRole",
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : "arn:aws:iam::*:policy/
AWSSystemsManagerJustInTimeAccessTokenPolicy"
        }
      }
    },
    {
      "Sid" : "IAMRoleManagementPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:GetRole",
        "iam:TagRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/SSM-JustInTimeAccessTokenRole"
      ],
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "QuickSetup*"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-JITNA"
          ]
        }
      }
    },
    {
      "Sid" : "ServiceSettingsManagementPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:servicesetting/ssm/just-in-time-access/identity-provider"
```

```
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSQuickSetupPatchPolicyBaselineAccess

説明: クイックセットアップを使用して、現在 AWS アカウント または組織の管理者が設定したパッチベースラインにアクセスするための読み取り専用アクセス許可を提供します。

AWSQuickSetupPatchPolicyBaselineAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSQuickSetupPatchPolicyBaselineAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 6 月 26 日 09:38 UTC
- 編集日時: 2024 年 6 月 26 日 09:38 UTC
- ARN: arn:aws:iam::aws:policy/AWSQuickSetupPatchPolicyBaselineAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "QuickSetupPatchingBaselineOverridesS3SameAccountReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::aws-quicksetup-patchpolicy-*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : [
            "${aws:ResourceAccount}"
          ]
        }
      }
    },
    {
      "Sid" : "QuickSetupPatchingBaselineOverridesS3OrganizationReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::aws-quicksetup-patchpolicy-*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalOrgID" : [
            "${aws:ResourceOrgID}"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSQuickSetupPatchPolicyDeploymentRolePolicy

説明: Quick Setup がパッチポリシー設定に関連付けられたリソースを作成できるようにするアクセス許可を提供します。

AWSQuickSetupPatchPolicyDeploymentRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSQuickSetupPatchPolicyDeploymentRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 6 月 26 日 09:57 UTC
- 編集日時: 2024 年 6 月 26 日 09:57 UTC
- ARN: arn:aws:iam::aws:policy/AWSQuickSetupPatchPolicyDeploymentRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackDriftDetectionStatus",
        "cloudformation:ListStacks"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CfnManage",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack",
        "cloudformation:DeleteStack",
        "cloudformation:CreateChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackResourceDrifts",
        "cloudformation:DetectStackDrift",
        "cloudformation:DetectStackResourceDrift"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/StackSet-AWS-QuickSetup-*"
      ]
    },
    {
      "Sid" : "RGroupsGet",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:GetGroupQuery"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "S3BucketsList",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
```

```
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AccessLogsBucketManage",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteBucketPolicy",
        "s3:Put*",
        "s3:Get*",
        "s3:List*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : [
        "arn:aws:s3:::aws-quicksetup-patchpolicy-access-log-*"
      ]
    },
    {
      "Sid" : "LambdaManage",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:UpdateFunction*",
        "lambda:GetFunction",
        "lambda:ListTags",
        "lambda:TagResource",
        "lambda:DeleteFunction",
        "lambda:InvokeFunction",
        "lambda:UntagResource"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
```

```
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : [
            "${aws:PrincipalAccount}"
          ]
        }
      },
      "Resource" : [
        "arn:aws:lambda:*:*:function:baseline-overrides-*",
        "arn:aws:lambda:*:*:function:delete-name-tags-*"
      ]
    },
    {
      "Sid" : "LogGroupsDescribe",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LogGroupsManage",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:TagResource",
        "logs:PutRetentionPolicy",
        "logs:DeleteLogGroup",
        "logs:ListTagsForResource",
        "logs:UntagResource"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/lambda/baseline-overrides-*",
        "arn:aws:logs:*:*:log-group:/aws/lambda/delete-name-tags-*"
```

```
      ]
    },
    {
      "Sid" : "QSDocsManage",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateDocument",
        "ssm:UpdateDocument",
        "ssm:DescribeDocument",
        "ssm:UpdateDocumentDefaultVersion",
        "ssm:DeleteDocument",
        "ssm:AddTagsToResource",
        "ssm:RemoveTagsFromResource",
        "ssm:ListTagsForResource"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSQuickSetup-*",
        "arn:aws:ssm:*:*:document/QuickSetup-*"
      ]
    },
    {
      "Sid" : "QSDocsGet",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSQuickSetup-*",
        "arn:aws:ssm:*:*:document/QuickSetup-*",
        "arn:aws:ssm:*::document/AWS-EnableExplorer",
        "arn:aws:ssm:*::document/AWS-RunPatchBaseline"
      ]
    },
    {
      "Sid" : "QSAssociationsManage",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ssm:CreateAssociation",
        "ssm:UpdateAssociation",
        "ssm:DeleteAssociation",
        "ssm:DescribeAssociation"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSQuickSetup-*",
        "arn:aws:ssm:*:*:document/QuickSetup-*",
        "arn:aws:ssm:*::document/AWS-EnableExplorer",
        "arn:aws:ssm:*::document/AWS-RunPatchBaseline",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*:*:association/*"
      ]
    },
    {
      "Sid" : "SSMSLRCreate",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ConfigRoleManage",
      "Effect" : "Allow",
      "Action" : [
        "iam:TagRole",
        "iam:UntagRole",
```

```
        "iam:GetRole",
        "iam:UpdateRole",
        "iam:DeleteRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:ListRoleTags"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-*"
      ]
    },
    {
      "Sid" : "ConfigRolePassToSSM",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ConfigRolePassToLambda",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lambda.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DocDescribe",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LegacyDocClean",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteDocument"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/QuickSetupID" : "*"
        }
      }
    },
    {
      "Sid" : "LegacyIAMClean",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole",
        "iam:DeleteRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/*QuickSetup-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/QuickSetupID" : "*"
        }
      }
    },
```

```
    {
      "Sid" : "ConfigRoleBoundedManage",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:AttachRolePolicy",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:PutRolePolicy",
        "iam:PutRolePermissionsBoundary"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/
AWSQuickSetupPatchPolicyPermissionsBoundary"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSQuickSetupPatchPolicyPermissionsBoundary

説明: QuickSetup は、ユーザーに代わって Systems Manager Patch Manager 機能を設定できるようにする IAM ロールを作成しますが、そのようなロール作成時にこのポリシーを使用してアクセス許可の範囲を定義します。

AWSQuickSetupPatchPolicyPermissionsBoundary は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSQuickSetupPatchPolicyPermissionsBoundary をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 6 月 26 日 09:46 UTC
- 編集日時: 2025 年 9 月 12 日 15:34 UTC
- ARN: arn:aws:iam::aws:policy/AWSQuickSetupPatchPolicyPermissionsBoundary

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PatchingAutomationRoleGetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
```

```
        "arn:aws:iam::*:role/AWS-QuickSetup-AutomationRole-*"
      ]
    },
    {
      "Sid" : "PatchingAutomationRolePassPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-AutomationRole-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DefaultInstanceRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:UpdateRole",
        "iam:GetRole"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:PrincipalTag/QuickSetupManagerID" : "*"
        },
        "ArnLike" : {
          "aws:PrincipalArn" : "arn:aws:iam::*:role/AWS-QuickSetup-AutomationRole-*"
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup"
      ]
    },
    {
      "Sid" : "DefaultInstanceRolePassPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PoliciesAttachPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore",
            "arn:aws:iam::aws:policy/AWSQuickSetupPatchPolicyBaselineAccess"
          ]
        },
        "StringLike" : {
          "aws:PrincipalTag/QuickSetupManagerID" : "*"
        },
        "ArnLike" : {
          "aws:PrincipalArn" : "arn:aws:iam::*:role/AWS-QuickSetup-AutomationRole-*"
        }
      },
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Sid" : "CreateSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
```

```
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "InstanceRoleAddPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:AddRoleToInstanceProfile"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ManagedInstanceRoleUpdatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateManagedInstanceRole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile",
        "iam:GetRolePolicy",
        "iam:ListInstanceProfilesForRole",
        "iam:ListRoles"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "InstanceProfileCreatePermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:CreateInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/AmazonSSMRoleForInstancesQuickSetup"
      ]
    },
    {
      "Sid" : "InstanceProfileAssociationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateIamInstanceProfile"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "ec2:InstanceProfile" : "true"
        },
        "ArnLike" : {
          "ec2:NewInstanceProfile" : "arn:aws:iam::*:instance-profile/
AmazonSSMRoleForInstancesQuickSetup"
        }
      }
    },
    {
      "Sid" : "InstanceProfileDisassociationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DisassociateIamInstanceProfile"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ec2:InstanceProfile" : "arn:aws:iam::*:instance-profile/
AmazonSSMRoleForInstancesQuickSetup"
        }
      }
    },
    {
      "Sid" : "SSMAssociationsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAssociationExecutions",
        "ssm:UpdateAssociation",
```

```
        "ssm:DescribeAssociation"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSQuickSetup-*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*:*:association/*"
      ]
    },
    {
      "Sid" : "BaselineS3Permissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:Put*",
        "s3:Get*",
        "s3:List*",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:DeleteBucket"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : [
            "${aws:PrincipalAccount}"
          ]
        }
      },
      "Resource" : "arn:aws:s3:::aws-quicksetup-patchpolicy-*"
    },
    {
      "Sid" : "PatchingFunctionsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:baseline-overrides-*",
        "arn:aws:lambda:*:*:function:delete-name-tags-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : [
            "${aws:PrincipalAccount}"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "LoggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/lambda/baseline-overrides-*",
        "arn:aws:logs:*:*:log-group:/aws/lambda/delete-name-tags-*"
      ]
    },
    {
      "Sid" : "SSMTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource",
        "ssm:RemoveTagsFromResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:managed-instance/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "QSConfigName-*"
        }
      }
    },
    {
      "Sid" : "EC2TaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "QSConfigName-*"
        }
      }
    },
```

```
    {
      "Sid" : "RoleTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:TagRole",
        "iam:UntagRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "QSConfigId-*"
        }
      }
    },
    {
      "Sid" : "PatchingReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetPatchBaseline",
        "ssm:GetInventory",
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeAssociation",
        "ssm:GetAutomationExecution",
        "ssm:ListTagsForResource",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PatchingAutomationsStartPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-definition/AWS-EnableExplorer*",
        "arn:aws:ssm:*:*:automation-definition/AWS-RunPatchBaseline*",
        "arn:aws:ssm:*:*:automation-definition/AWS-AttachIAMToInstance*",
        "arn:aws:ssm:*:*:automation-definition/QuickSetup-*",
        "arn:aws:ssm:*:*:automation-definition/AWSQuickSetup-*",
        "arn:aws:ssm:*:*:document/AWS-EnableExplorer*",
        "arn:aws:ssm:*:*:document/AWS-RunPatchBaseline*",
        "arn:aws:ssm:*:*:document/AWS-AttachIAMToInstance*",
```

```
        "arn:aws:ssm:*:*:document/QuickSetup-*",
        "arn:aws:ssm:*:*:document/AWSQuickSetup-*",
        "arn:aws:ssm:*:*:automation-execution/*"
      ]
    },
    {
      "Sid" : "ReadOnlyPermissionsForEnablingExplorer",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "config:DescribeConfigurationRecorders",
        "compute-optimizer:GetEnrollmentStatus",
        "support:DescribeTrustedAdvisorChecks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ExplorerServiceSettingsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/ssm-patchmanager",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/EC2",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ExplorerOnboarded",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/Association",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ComputeOptimizer",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ConfigCompliance",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/OpsData-TrustedAdvisor",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/SupportCenterCase"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSQuickSetupSchedulerPermissionsBoundary

説明: AWSQuickSetupSchedulerPermissionsBoundary ポリシーは、Quick Setup によって作成された IAM ロールに付与されるアクセス許可のリストを定義します。Quick Setup では、このポリシーで作成されたロールを使用して、Amazon EC2 インスタンスや他のリソースでスケジュールされたオペレーションを有効にして設定します。

AWSQuickSetupSchedulerPermissionsBoundary は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSQuickSetupSchedulerPermissionsBoundary をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 6 月 26 日 09:53 UTC
- 編集日時: 2024 年 6 月 26 日 09:53 UTC
- ARN: arn:aws:iam::aws:policy/AWSQuickSetupSchedulerPermissionsBoundary

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-Scheduler-*"
      ]
    },
    {
      "Sid" : "ConfigurationAutomationRolePassPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-Scheduler-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "SystemsManagerCalendarReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetCalendarState"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSQuickSetup-ChangeCalendar-*"
      ]
    },
    {
      "Sid" : "EC2ReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeRegions",
        "ec2:DescribeTags",
        "tag:GetResources"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "EC2StartStopPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AutomationStartPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-definition/AWSQuickSetup-
StartStateManagerAssociations-*"
      ]
    },
    {
      "Sid" : "AssociationsStartOncePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAssociationsOnce"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:association/*"
      ]
    },
    {
      "Sid" : "CreateSystemsManagerSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
```

```
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ReadOnlyPermissionsForEnablingExplorer",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "config:DescribeConfigurationRecorders",
        "compute-optimizer:GetEnrollmentStatus",
        "support:DescribeTrustedAdvisorChecks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMExplorerServiceSettingsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/ssm-patchmanager",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/EC2",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ExplorerOnboarded",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/Association",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ComputeOptimizer",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ConfigCompliance",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/OpsData-TrustedAdvisor",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/SupportCenterCase"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSQuickSetupSSMDeploymentRolePolicy

説明: このポリシーは、Systems Manager のオンボーディングプロセス時に使用されるリソースの作成を Quick Setup に許可する管理アクセス許可を付与します。

AWSQuickSetupSSMDeploymentRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSQuickSetupSSMDeploymentRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 11 月 15 日 22:53 UTC
- 編集日時: 2025 年 10 月 27 日 11:49 UTC
- ARN: arn:aws:iam::aws:policy/AWSQuickSetupSSMDeploymentRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackDriftDetectionStatus",
        "cloudformation:ListStacks"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack",
        "cloudformation:DeleteStack",
        "cloudformation:CreateChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackResourceDrifts",
        "cloudformation:DetectStackDrift",
        "cloudformation:DetectStackResourceDrift",
        "cloudformation:DescribeStackEvents"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/StackSet-AWS-QuickSetup-SSM-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:TagResource"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : [
            "${aws:PrincipalAccount}"
          ],
          "aws:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM"
          ],
          "aws:RequestTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM"
          ]
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "QuickSetup*"
          ]
        }
      },
      "Resource" : [
        "arn:aws:lambda:*:*:function:aws-quicksetup-lifecycle*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction",
        "lambda:DeleteFunction",
        "lambda:UpdateFunction*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : [
            "${aws:PrincipalAccount}"
          ],
          "aws:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM"
          ]
        }
      },
      "Resource" : [
```

```
        "arn:aws:lambda:*:*:function:aws-quicksetup-lifecycle*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetFunction"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cloudformation.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : "arn:aws:lambda:*:*:function:aws-quicksetup-lifecycle*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:UpdateAssociation",
        "ssm:DeleteAssociation",
        "ssm:DescribeAssociation",
        "ssm:GetDocument",
        "ssm:DescribeDocument"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ssm:*::document/AWSQuickSetupType-EnableAREX",
        "arn:aws:ssm:*::document/AWSQuickSetupType-EnableDHMC",
        "arn:aws:ssm:*::document/AWSQuickSetupType-ManageInstanceProfile",
        "arn:aws:ssm:*::document/AWS-EnableExplorer",
        "arn:aws:ssm:*::document/AWS-GatherSoftwareInventory",
        "arn:aws:ssm:*::document/AWS-UpdateSSMAgent",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:managed-instance/*",
```

```
        "arn:aws:ssm:*:*:association/*"
      ]
    },
    {
      "Sid" : "SSMSLRCreate",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:TagRole"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "QuickSetup*"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM"
          ],
          "aws:RequestTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM"
          ]
        }
```

```
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-*",
        "arn:aws:iam::*:role/AWS-SSM-Remediation*",
        "arn:aws:iam::*:role/AWS-SSM-Diagnosis*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:UpdateRole",
        "iam:DeleteRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:ListRoleTags"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-*",
        "arn:aws:iam::*:role/AWS-SSM-Remediation*",
        "arn:aws:iam::*:role/AWS-SSM-Diagnosis*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/
AWSQuickSetupSSMLifecycleManagementExecutionPolicy"
          ]
        }
```

```
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-LifecycleManagement-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : "arn:aws:iam::aws:policy/
AWSQuickSetupSSMManageResourcesExecutionPolicy"
        }
      },
      "Resource" : "arn:aws:iam::*:role/AWS-QuickSetup-SSM-ManageResources-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/AWS-SSM-RemediationAutomation-
AdministrationRolePolicy",
            "arn:aws:iam::aws:policy/AWS-SSM-RemediationAutomation-
ExecutionRolePolicy",
            "arn:aws:iam::aws:policy/AWS-SSM-RemediationAutomation-
OperationalAccountAdministrationRolePolicy",
            "arn:aws:iam::aws:policy/AWS-SSM-Automation-DiagnosisBucketPolicy",
            "arn:aws:iam::aws:policy/AWS-SSM-DiagnosisAutomation-
AdministrationRolePolicy",
            "arn:aws:iam::aws:policy/AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy"
          ]
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWS-SSM-Remediation*",
        "arn:aws:iam::*:role/AWS-SSM-Diagnosis*"
```

```
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com",
          "iam:ResourceTag/QuickSetupDocument" : "AWSQuickSetupType-SSM"
        },
        "ArnLike" : {
          "iam:AssociatedResourceARN" : [
            "arn:aws:ssm:*::document/AWSQuickSetupType-EnableAREX",
            "arn:aws:ssm:*::document/AWSQuickSetupType-EnableDHMC",
            "arn:aws:ssm:*::document/AWSQuickSetupType-ManageInstanceProfile",
            "arn:aws:ssm:*::document/AWS-EnableExplorer",
            "arn:aws:ssm:*:*:association/*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-LifecycleManagement*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "lambda.amazonaws.com",
          "iam:ResourceTag/QuickSetupDocument" : "AWSQuickSetupType-SSM"
        },
        "ArnLike" : {
          "iam:AssociatedResourceARN" : [
            "arn:aws:lambda:*:*:function:aws-quicksetup-lifecycle-*"
          ]
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "lambda:TagResource",
      "Resource" : [
        "arn:aws:lambda:*:*:function:aws-quicksetup-lifecycle*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cloudformation.amazonaws.com"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "QuickSetup*"
        },
        "StringLike" : {
          "aws:RequestTag/QuickSetupDocumentVersionName" : "*"
        },
        "StringEquals" : {
          "aws:ResourceTag/QuickSetupDocument" : "AWSQuickSetupType-SSM"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:TagRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-*",
        "arn:aws:iam::*:role/AWS-SSM-Remediation*",
        "arn:aws:iam::*:role/AWS-SSM-Diagnosis*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cloudformation.amazonaws.com"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "QuickSetup*"
        },
        "StringLike" : {
          "aws:RequestTag/QuickSetupDocumentVersionName" : "*"
        },
        "StringEquals" : {
```

```
          "aws:ResourceTag/QuickSetupDocument" : "AWSQuickSetupType-SSM"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:AddTagsToResource"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:association/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:UpdateAssociation",
        "ssm:DeleteAssociation",
        "ssm:DescribeAssociation"
      ],
      "Resource" : "arn:aws:ssm:*::document/AWSQuickSetupType-SSM-ManageResources"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateAssociation",
        "ssm:DeleteAssociation",
        "ssm:DescribeAssociation"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:association/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/QuickSetupDocument" : [
```

```
            "AWSQuickSetupType-SSM"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource",
        "ssm:RemoveTagsFromResource"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:association/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAssociationExecutions",
        "ssm:DescribeAssociationExecutionTargets",
        "ssm:GetAutomationExecution"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ssm:*:*:automation-execution/*",
```

```
        "arn:aws:ssm:*:*:association/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/AWS-QuickSetup-SSM-ManageResources*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ],
          "iam:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSQuickSetupSSMDeploymentS3BucketRolePolicy

説明: このポリシーは、アカウント内のすべての S3 バケットを一覧表示し、 AWS CloudFormation テンプレートを通じて管理されるプリンシパルアカウントの特定のバケットに関する情報を管理および取得するためのアクセス許可を付与します。

AWSQuickSetupSSMDeploymentS3BucketRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSQuickSetupSSMDeploymentS3BucketRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 11 月 15 日 22:01 UTC
- 編集日時: 2024 年 11 月 15 日 22:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupSSMDeploymentS3BucketRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteBucketPolicy",
        "s3:PutBucketPublicAccessBlock",
        "s3:ListBucket",
        "s3:PutBucketPolicy",
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketTagging",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketVersioning"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cloudformation.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      },
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSQuickSetupSSMHostMgmtPermissionsBoundary

説明: Quick Setup は、ユーザーに代わって Host Manager Quick Setup タイプを設定できるようにする IAM ロールを作成しますが、そのようなロール作成時にこのポリシーを使用してアクセス許可の範囲を定義します。

`AWSQuickSetupSSMHostMgmtPermissionsBoundary` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSQuickSetupSSMHostMgmtPermissionsBoundary` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 6 月 26 日 09:48 UTC
- 編集日時: 2024 年 6 月 26 日 09:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupSSMHostMgmtPermissionsBoundary`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "HostManagementAutomationRoleGetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-HostMgmtRole-*"
      ]
    },
    {
      "Sid" : "HostManagementAutomationRolePassPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-HostMgmtRole-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DefaultInstanceRoleManagePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:UpdateRole",
```

```
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:PrincipalTag/QuickSetupManagerID" : "*"
        },
        "ArnLike" : {
          "aws:PrincipalArn" : "arn:aws:iam::*:role/AWS-QuickSetup-HostMgmtRole-*"
        }
      }
    },
    {
      "Sid" : "DefaultInstanceRolePassToEC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DefaultInstanceRolePassToSSMPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "InstanceManagementPoliciesAttachPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore",
            "arn:aws:iam::aws:policy/AmazonSSMPatchAssociation"
          ]
        },
        "StringLike" : {
          "aws:PrincipalTag/QuickSetupManagerID" : "*"
        },
        "ArnLike" : {
          "aws:PrincipalArn" : "arn:aws:iam::*:role/AWS-QuickSetup-HostMgmtRole-*"
        }
      },
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Sid" : "CreateSystemsManagerSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
      }
    },
    {
```

```
      "Sid" : "DefaultInstanceRoleAddPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:AddRoleToInstanceProfile"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "IAMReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile",
        "iam:GetRolePolicy",
        "iam:ListInstanceProfilesForRole",
        "iam:ListRoles"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DefaultInstanceProfileCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/AmazonSSMRoleForInstancesQuickSetup"
      ]
    },
    {
      "Sid" : "DefaultInstanceProfileAssociationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateIamInstanceProfile"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "ec2:InstanceProfile" : "true"
        },
        "ArnLike" : {
```

```
          "ec2:NewInstanceProfile" : "arn:aws:iam::*:instance-profile/
AmazonSSMRoleForInstancesQuickSetup"
        }
      }
    },
    {
      "Sid" : "DefaultInstanceProfileDisassociationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DisassociateIamInstanceProfile"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ec2:InstanceProfile" : "arn:aws:iam::*:instance-profile/
AmazonSSMRoleForInstancesQuickSetup"
        }
      }
    },
    {
      "Sid" : "ConfigurationAutomationsStartPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-definition/AWSQuickSetup-HostMgmt-*",
        "arn:aws:ssm:*:*:automation-definition/AWSQuickSetup-
CreateAndAttachIAMToInstance-*",
        "arn:aws:ssm:*:*:automation-definition/AWSQuickSetup-
UpdateExistingInstanceProfile-*",
        "arn:aws:ssm:*:*:automation-definition/AWSQuickSetup-
InstallAndManageCloudWatchDocument-*",
        "arn:aws:ssm:*:*:automation-definition/UpdateCloudWatchDocument-*",
        "arn:aws:ssm:*:*:automation-definition/AWSEC2-UpdateLaunchAgent-*",
        "arn:aws:ssm:*:*:automation-definition/AWS-AttachIAMToInstance*",
        "arn:aws:ssm:*:*:automation-definition/AWS-GatherSoftwareInventory*",
        "arn:aws:ssm:*:*:automation-definition/AWS-RunPatchBaselineAssociation*",
        "arn:aws:ssm:*:*:automation-definition/AWS-UpdateSSMAgent*"
      ]
    },
    {
      "Sid" : "ReadOnlyPermissionsForEnablingHostManagementBySSM",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ssm:ListTagsForResource",
        "ssm:GetAutomationExecution",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ReadOnlyPermissionsForEnablingExplorer",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigurationRecorders",
        "compute-optimizer:GetEnrollmentStatus",
        "support:DescribeTrustedAdvisorChecks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMExplorerServiceSettingsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/ssm-patchmanager",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/EC2",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ExplorerOnboarded",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/Association",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ComputeOptimizer",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ConfigCompliance",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/OpsData-TrustedAdvisor",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/SupportCenterCase"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSQuickSetupSSMLifecycleManagementExecutionPolicy

説明: このポリシーは、Systems Manager での高速セットアップデプロイ中にライフサイクルイベントでクイックセットアップが a AWS CloudFormation カスタムリソースを実行できるようにする管理アクセス許可を付与します。

`AWSQuickSetupSSMLifecycleManagementExecutionPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSQuickSetupSSMLifecycleManagementExecutionPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 11 月 15 日 21:55 UTC
- 編集日時: 2025 年 9 月 12 日 15:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupSSMLifecycleManagementExecutionPolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/QuickSetupDocument" : "AWSQuickSetupType-SSM"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/AWS-QuickSetup-SSM-ManageResources*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ],
          "iam:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution",
        "ssm:AddTagsToResource"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-definition/AWSQuickSetupType-SSM-ManageResources*",
        "arn:aws:ssm:*:*:document/AWSQuickSetupType-SSM-ManageResources*",
        "arn:aws:ssm:*:*:automation-execution/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/QuickSetupDocument" : "AWSQuickSetupType-SSM",
          "aws:ResourceTag/QuickSetupDocument" : "AWSQuickSetupType-SSM"
        }
      }
```

```
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSQuickSetupSSMManageResourcesExecutionPolicy

説明: このポリシーは、Systems Manager が Systems Manager のオンボーディングに必要な IAM ロールなどの前提条件を作成できるようにするアクセス許可を付与します。

`AWSQuickSetupSSMManageResourcesExecutionPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSQuickSetupSSMManageResourcesExecutionPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 11 月 15 日 22:49 UTC
- 編集日時: 2024 年 11 月 15 日 22:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupSSMManageResourcesExecutionPolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:TagRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-EnableExplorer*",
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-EnableDHMC*",
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-ManageInstanceProfile*",
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-EnableAREX*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:ResourceTag/QuickSetupDocument" : "AWSQuickSetupType-SSM",
          "aws:RequestTag/QuickSetupDocument" : "AWSQuickSetupType-SSM"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:UpdateRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-EnableExplorer*",
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-EnableDHMC*",
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-ManageInstanceProfile*",
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-EnableAREX*"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/AWSSystemsManagerEnableExplorerExecutionPolicy"
          ]
        }
      },
      "Resource" : "arn:aws:iam::*:role/AWS-QuickSetup-SSM-EnableExplorer*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : "arn:aws:iam::aws:policy/
AWSQuickSetupEnableDHMCExecutionPolicy"
        }
      },
      "Resource" : "arn:aws:iam::*:role/AWS-QuickSetup-SSM-EnableDHMC*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : "arn:aws:iam::aws:policy/
AWSQuickSetupManagedInstanceProfileExecutionPolicy"
        }
      },
      "Resource" : "arn:aws:iam::*:role/AWS-QuickSetup-SSM-ManageInstanceProfile*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : "arn:aws:iam::aws:policy/
AWSQuickSetupEnableAREXExecutionPolicy"
        }
      },
      "Resource" : "arn:aws:iam::*:role/AWS-QuickSetup-SSM-EnableAREX*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteObject",
        "s3:ListBucketVersions",
        "s3:DeleteObjectVersion",
        "s3:GetObjectVersion",
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : [
            "${aws:PrincipalAccount}"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSQuickSetupStartSSMAssociationsExecutionPolicy

説明: このポリシーは、プリンシパルがステートマネージャーの関連付けを開始する AWSQuickSetupType-StartSSMAssociations Automation ランブックを実行できるようにするアクセス許可を付与します。

`AWSQuickSetupStartSSMAssociationsExecutionPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSQuickSetupStartSSMAssociationsExecutionPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 8 月 8 日 12:04 UTC
- 編集日時: 2025 年 9 月 12 日 14:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupStartSSMAssociationsExecutionPolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSQuickSetupType-Scheduler-ChangeCalendarState",
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:automation-definition/AWSQuickSetupType-Scheduler-
ChangeCalendarState*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        },
        "ArnLike" : {
          "iam:AssociatedResourceARN" : [
            "arn:aws:ssm:*:*:document/AWSQuickSetupType-Scheduler-ChangeCalendarState",
            "arn:aws:ssm:*:*:automation-definition/AWSQuickSetupType-Scheduler-
ChangeCalendarState*"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSQuickSetupStartStopInstancesExecutionPolicy

説明: マネージドポリシー AWSQuickSetupStartStopInstancesExecutionPolicy は、Quick Setup がスケジュールに従って Amazon EC2 インスタンスを起動および停止するためのアクセス許可を提供します。このポリシーは、Quick Setup スケジューラの設定タイプで使用されます。

`AWSQuickSetupStartStopInstancesExecutionPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSQuickSetupStartStopInstancesExecutionPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 8 月 8 日 12:04 UTC
- 編集日時: 2025 年 9 月 12 日 15:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupStartStopInstancesExecutionPolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
```

```
        "ec2:DescribeRegions",
        "ec2:DescribeTags"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetCalendarState"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/AWSQuickSetup-ChangeCalendar*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAssociationsOnce",
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:association/*",
        "arn:aws:ssm:*:*:document/AWSQuickSetupType-Scheduler-ApplyInstanceState",
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:automation-definition/AWSQuickSetupType-Scheduler-
ApplyInstanceState*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
```

```
          ]
        },
        "ArnLike" : {
          "iam:AssociatedResourceARN" : [
            "arn:aws:ssm:*::document/AWSQuickSetupType-Scheduler-ApplyInstanceState",
            "arn:aws:ssm:*:*:association/*"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSQuickSightAssetBundleExportPolicy

説明: QuickSight アセットバンドルエクスポートオペレーションの実行に必要な一連のアクセス許可を提供します。

`AWSQuickSightAssetBundleExportPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSQuickSightAssetBundleExportPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 3 月 27 日 21:31 UTC
- 編集日時: 2024 年 3 月 27 日 21:31 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSightAssetBundleExportPolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSQuickSightAssetBundleImportPolicy

説明: QuickSight アセットバンドルインポートオペレーションの実行に必要な一連のアクセス許可を提供

AWSQuickSightAssetBundleImportPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSQuickSightAssetBundleImportPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 3 月 27 日 21:40 UTC
- 編集日時: 2024 年 3 月 27 日 21:40 UTC
- ARN: arn:aws:iam::aws:policy/AWSQuickSightAssetBundleImportPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSQuicksightAthenaAccess

説明: Athena のクエリ結果に使用される Athena API および S3 バケットへの Quicksight アクセス

`AWSQuicksightAthenaAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSQuicksightAthenaAccess` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2016 年 12 月 9 日 02:31 UTC
- 編集日時: 2025 年 1 月 3 日 00:22 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuicksightAthenaAccess`

ポリシーのバージョン

ポリシーのバージョン: v11 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "athena:BatchGetQueryExecution",
        "athena:CancelQueryExecution",
        "athena:GetCatalogs",
        "athena:GetExecutionEngine",
        "athena:GetExecutionEngines",
        "athena:GetNamespace",
        "athena:GetNamespaces",
        "athena:GetQueryExecution",
        "athena:GetQueryExecutions",
        "athena:GetQueryResults",
        "athena:GetQueryResultsStream",
        "athena:GetTable",
        "athena:GetTables",
        "athena:ListQueryExecutions",
        "athena:RunQuery",
        "athena:StartQueryExecution",
        "athena:StopQueryExecution",
        "athena:ListWorkGroups",
        "athena:ListEngineVersions",
        "athena:GetWorkGroup",
        "athena:GetDataCatalog",
        "athena:GetDatabase",
        "athena:GetTableMetadata",
        "athena:ListDataCatalogs",
        "athena:ListDatabases",
        "athena:ListTableMetadata"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:DeleteDatabase",
        "glue:GetCatalog",
        "glue:GetCatalogs",
        "glue:GetDatabase",
```

```
        "glue:GetDatabases",
        "glue:UpdateDatabase",
        "glue:CreateTable",
        "glue:DeleteTable",
        "glue:BatchDeleteTable",
        "glue:UpdateTable",
        "glue:GetTable",
        "glue:GetTables",
        "glue:BatchCreatePartition",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
        "glue:UpdatePartition",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:BatchGetPartition"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:ListMultipartUploadParts",
        "s3:AbortMultipartUpload",
        "s3:CreateBucket",
        "s3:PutObject",
        "s3:PutBucketPublicAccessBlock"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-athena-query-results-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataAccess"
      ],
      "Resource" : [
```

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSQuickSightDescribeRDS

説明: QuickSight が RDS リソースを記述できるようにします

AWSQuickSightDescribeRDS は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSQuickSightDescribeRDS をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 11 月 10 日 23:24 UTC
- 編集日時: 2015 年 11 月 10 日 23:24 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSQuickSightDescribeRDS

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSQuickSightDescribeRedshift

説明: QuickSight が Redshift リソースを記述できるようにします

`AWSQuickSightDescribeRedshift` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSQuickSightDescribeRedshift` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 11 月 10 日 23:25 UTC
- 編集日時: 2015 年 11 月 10 日 23:25 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSQuickSightElasticsearchPolicy

説明: Amazon QuickSight からの Amazon Elastic 検索リソースへのアクセスを提供します

`AWSQuickSightElasticsearchPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSQuickSightElasticsearchPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 9 月 9 日 17:27 UTC
- 編集日時: 2021 年 9 月 7 日 23:25 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSQuickSightElasticsearchPolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSQuickSightIoTAnalyticsAccess

説明: QuickSight に IoT 分析データセットへの読み取り専用アクセスを付与します

AWSQuickSightIoTAnalyticsAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSQuickSightIoTAnalyticsAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 11 月 29 日 17:00 UTC
- 編集日時: 2017 年 11 月 29 日 17:00 UTC
- ARN: arn:aws:iam::aws:policy/AWSQuickSightIoTAnalyticsAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSQuickSightListIAM

説明: QuickSight に IAM エンティティを一覧表示できるようにします

AWSQuickSightListIAM は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSQuickSightListIAM をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 11 月 10 日 23:25 UTC
- 編集日時: 2015 年 11 月 10 日 23:25 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSQuickSightListIAM

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSQuicksightOpenSearchPolicy

説明: Amazon QuickSight からの Amazon OpenSearch リソースへのアクセスを提供します

`AWSQuicksightOpenSearchPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSQuicksightOpenSearchPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2021 年 9 月 7 日 23:26 UTC
- 編集日時: 2021 年 9 月 7 日 23:26 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuicksightOpenSearchPolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
```

```
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSQuickSightSageMakerPolicy

説明: Amazon QuickSight からの Amazon SageMaker のリソースへのアクセスを提供します

`AWSQuickSightSageMakerPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSQuickSightSageMakerPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 1 月 17 日 17:18 UTC
- 編集日時: 2023 年 10 月 30 日 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightSageMakerPolicy`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSQuickSightSecretsManagerWriteAccess

説明: QuickSight が AWS Secrets Manager でシークレットを作成し、既存の QuickSight シークレットにリソースポリシーをアタッチするために使用するポリシー。

`AWSQuickSightSecretsManagerWriteAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSQuickSightSecretsManagerWriteAccess` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2025 年 5 月 22 日 01:22 UTC
- 編集日時: 2025 年 5 月 22 日 01:22 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightSecretsManagerWriteAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:PutResourcePolicy"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:quicksight!*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "quicksight",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:quicksight!*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "secretsmanager:Name" : "quicksight!*"
        }
      }
    }
  ]
```

```
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSQuickSightSecretsManagerWritePolicy

説明: QuickSight が AWS Secrets Manager でシークレットを作成し、既存の QuickSight シークレットにリソースポリシーをアタッチするために使用するポリシー。

`AWSQuickSightSecretsManagerWritePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSQuickSightSecretsManagerWritePolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 5 月 12 日 19:22 UTC
- 編集日時: 2025 年 5 月 12 日 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSightSecretsManagerWritePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:PutResourcePolicy"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:quicksight!*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "quicksight",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:quicksight!*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "secretsmanager:Name" : "quicksight!*"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSQuickSightTimestreamPolicy

説明: AWS Timestream APIsへの AWS QuickSight アクセス。お客様は、このポリシーを AWS QuickSight ロールにアタッチして、データとメタデータの取得を許可できます。

AWSQuickSightTimestreamPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSQuickSightTimestreamPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 9 月 30 日 21:47 UTC
- 編集日時: 2020 年 9 月 30 日 21:47 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSQuickSightTimestreamPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSReachabilityAnalyzerServiceRolePolicy

説明: VPC Reachability Analyzer がユーザーに代わって AWS リソースにアクセスし、 AWS Organizations と統合できるようにします。

`AWSReachabilityAnalyzerServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 11 月 23 日 17:12 UTC
- 編集日時: 2024 年 9 月 10 日 16:04 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReachabilityAnalyzerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAssociations",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualGateways",
        "directconnect:DescribeVirtualInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTransitGatewayAttachments",
```

```
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:SearchTransitGatewayRoutes",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListAccounts",
        "organizations:ListDelegatedAdministrators",
        "resource-groups:ListGroups",
        "resource-groups:ListGroupResources",
        "tag:GetResources",
        "tiros:CreateQuery",
        "tiros:ExtendQuery",
        "tiros:GetQueryAnswer",
        "tiros:GetQueryExplanation",
        "tiros:GetQueryExtensionAccounts"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "ApigatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/vpclinks"
      ]
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSRefactoringToolkitFullAccess

説明: このポリシーは、Microsoft Visual Studio の AWS Toolkit for .NET リファクタリング拡張機能で AWS サービスを使用するアクセス許可を付与します。ローカル AWS プロファイルにアタッチすることを目的としています。このポリシーにより、アプリケーションアーティファクトのアップロードし、Amazon S3 からの結果のアーティファクトをダウンロードできます。これにより、 AWS CodeBuild を使用してアプリケーションをコンテナイメージに構築し、Amazon Elastic Container Registry (Amazon ECR) からイメージを保存および取得できます。また、Amazon Elastic Container Service (Amazon ECS) AWS などの のコンテナサービスへのアプリケーションのデプロイ、VPC リソースのオプションの作成、 AWS ディレクトリサービスなどの既存のインフラストラクチャへのオプションの接続、およびその他の関連サービスが可能になります。

`AWSRefactoringToolkitFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSRefactoringToolkitFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 10 月 25 日 16:41 UTC
- 編集日時: 2025 年 4 月 9 日 20:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRefactoringToolkitFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "a2c:GetContainerizationJobDetails",
        "a2c:GetDeploymentJobDetails",
        "a2c:StartContainerizationJob",
        "a2c:StartDeploymentJob"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:CreateStack",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:UpdateStack",
        "cloudformation:TagResource",
```

```
        "cloudformation:UntagResource"
      ],
      "Resource" : [
        "arn:*:cloudformation:*:*:stack/a2c-app-*",
        "arn:*:cloudformation:*:*:stack/a2c-build-*",
        "arn:*:cloudformation:*:*:stack/application-transformation-app-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "codebuild:CreateProject",
        "codebuild:UpdateProject"
      ],
      "Resource" : "arn:aws:codebuild:*:*:project/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "codebuild:StartBuild"
      ],
      "Resource" : "arn:aws:codebuild:*:*:project/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateInternetGateway",
        "ec2:CreateKeyPair",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSubnet",
        "ec2:CreateVpc",
```

```
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateInternetGateway",
        "ec2:CreateKeyPair",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSubnet",
        "ec2:CreateVpc",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/application-transformation" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "application-transformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:CreateTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "AuthorizeSecurityGroupIngress",
            "CreateInternetGateway",
            "CreateKeyPair",
            "CreateRoute",
            "CreateRouteTable",
            "CreateSubnet",
            "CreateVpc"
          ]
        },
        "Null" : {
          "aws:RequestTag/application-transformation" : "false"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "application-transformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateRouteTable",
        "ec2:AttachInternetGateway",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteTags",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateSubnet",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/a2c-generated" : "false"
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateRouteTable",
        "ec2:AttachInternetGateway",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteTags",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateSubnet",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/application-transformation" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository",
        "ecr:TagResource"
      ],
      "Resource" : "arn:*:ecr:*:*:repository/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository",
        "ecr:TagResource"
      ],
      "Resource" : "arn:*:ecr:*:*:repository/*",
      "Condition" : {
```

```
        "Null" : {
          "aws:RequestTag/application-transformation" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetLifecyclePolicy",
        "ecr:GetRepositoryPolicy",
        "ecr:ListImages",
        "ecr:ListTagsForResource",
        "ecr:TagResource",
        "ecr:UntagResource"
      ],
      "Resource" : "arn:*:ecr:*:*:repository/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetLifecyclePolicy",
        "ecr:GetRepositoryPolicy",
        "ecr:ListImages",
        "ecr:ListTagsForResource",
        "ecr:TagResource",
        "ecr:UntagResource"
      ],
      "Resource" : "arn:*:ecr:*:*:repository/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/application-transformation" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:CreateCluster",
        "ecs:CreateService",
```

```
        "ecs:RegisterTaskDefinition",
        "ecs:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:CreateCluster",
        "ecs:CreateService",
        "ecs:RegisterTaskDefinition",
        "ecs:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/application-transformation" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:UpdateService",
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:UpdateService",
        "ecs:TagResource",
```

```
        "ecs:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/application-transformation" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeTaskDefinition"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cloudformation.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:ExecuteCommand"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ecs:container-name" : "a2c-sidecar"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:ExecuteCommand"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ecs:container-name" : "application-transformation-sidecar"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/ecs.amazonaws.com/
AWSServiceRoleForECS",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "ecs.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:TagResource"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/codebuild/*:*",
        "arn:aws:logs:*:*:log-group:/aws/ecs/containerinsights/*:*",
        "arn:aws:logs:*:*:log-group:/aws/ecs/container-logs/*:*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/a2c-generated" : "false"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "a2c-generated"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:TagResource"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/ecs/containerinsights/*:*",
        "arn:aws:logs:*:*:log-group:/aws/ecs/container-logs/*:*"
      ],
```

```
      "Condition" : {
        "Null" : {
          "aws:RequestTag/application-transformation" : "false"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "application-transformation"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:GetLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/codebuild/*:*",
        "arn:aws:logs:*:*:log-group:/aws/ecs/containerinsights/*:*",
        "arn:aws:logs:*:*:log-group:/aws/ecs/container-logs/*:*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:GetLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/ecs/containerinsights/*:*",
        "arn:aws:logs:*:*:log-group:/aws/ecs/container-logs/*:*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/application-transformation" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ssm:AddTagsToResource",
        "ssm:GetParameters",
        "ssm:PutParameter",
        "ssm:RemoveTagsFromResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/a2c-generated-check-ecs-slr-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeSessions",
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*/refactoringtoolkit*",
        "arn:aws:s3:::*/a2c-generated*",
        "arn:aws:s3:::*/application-transformation*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringLike" : {
          "s3:prefix" : [
            "application-transformation",
            "refactoringtoolkit"
          ]
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks",
        "clouddirectory:ListDirectories",
        "codebuild:BatchGetProjects",
        "codebuild:BatchGetBuilds",
        "ds:DescribeDirectories",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeRegions",
        "ecr:DescribeImages",
        "ecr:DescribeRepositories",
        "ecs:DescribeClusters",
        "ecs:DescribeServices",
        "ecs:DescribeTasks",
        "ecs:ListTagsForResource",
        "ecs:ListTasks",
        "iam:ListRoles",
        "s3:GetBucketLocation",
        "s3:GetBucketVersioning",
        "s3:ListAllMyBuckets",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/ecs.amazonaws.com/
AWSServiceRoleForECS"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws.portingassistant.dotnet.datastore",
        "arn:aws:s3:::aws.portingassistant.dotnet.datastore/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "application-transformation:StartPortingCompatibilityAssessment",
        "application-transformation:GetPortingCompatibilityAssessment",
        "application-transformation:StartPortingRecommendationAssessment",
        "application-transformation:GetPortingRecommendationAssessment",
        "application-transformation:PutLogData",
        "application-transformation:PutMetricData",
        "application-transformation:StartContainerization",
        "application-transformation:GetContainerization",
        "application-transformation:StartDeployment",
        "application-transformation:GetDeployment"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:DescribeKey",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*::*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "kms:ResourceAliases" : "alias/application-transformation*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "ecr:InitiateLayerUpload",
        "ecr:PutImage",
        "ecr:UploadLayerPart",
        "ecr:CompleteLayerUpload",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer"
      ],
      "Resource" : "arn:*:ecr:*:*:repository/*",
      "Condition" : {
        "Null" : {
          "ecr:ResourceTag/application-transformation" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:aws:kms:*::*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        },
        "ForAnyValue:StringLike" : {
          "kms:ResourceAliases" : "alias/application-transformation*"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSRefactoringToolkitSidecarPolicy

説明: このポリシーは、Microsoft Visual Studio 用の AWS Toolkit for .NET リファクタリング拡張機能 AWS を使用して でアプリケーションをテストするために作成された Amazon ECS タスクで使用することを目的としています。このポリシーは、Amazon S3 からのアプリケーションアーティファクトのダウンロード、 AWS Systems Manager を使用したタスクのステータスの通信、およびその他の必要なサービスへのアクセスを許可します。

`AWSRefactoringToolkitSidecarPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSRefactoringToolkitSidecarPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 10 月 25 日 16:41 UTC
- 編集日時: 2022 年 10 月 29 日 22:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRefactoringToolkitSidecarPolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSrePostPrivateCloudWatchAccess

説明: CloudWatch メトリクスデータを公開するための re:Post Private アクセスを提供します

AWSrePostPrivateCloudWatchAccess は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 11 月 15 日 16:37 UTC
- 編集日時: 2023 年 11 月 15 日 16:37 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSrePostPrivateCloudWatchAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/rePostPrivate",
            "AWS/Usage"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSRepostSpaceSupportOperationsPolicy

説明: このポリシーにより、re:Post Space サービスは、Space アプリケーションを通じて作成されるサポートケースを作成、管理、解決できます。

AWSRepostSpaceSupportOperationsPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSRepostSpaceSupportOperationsPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 11 月 26 日 21:52 UTC
- 編集日時: 2023 年 11 月 26 日 21:52 UTC
- ARN: arn:aws:iam::aws:policy/AWSRepostSpaceSupportOperationsPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RepostSpaceSupportOperations",
      "Effect" : "Allow",
      "Action" : [
        "support:AddAttachmentsToSet",
        "support:AddCommunicationToCase",
        "support:CreateCase",
        "support:DescribeCases",
        "support:DescribeCommunications",
        "support:ResolveCase"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSResilienceHubAsssessmentExecutionPolicy

説明: 評価を実行するために他の サービスへのアクセスを許可する AWS Resilience Hub AWS サービスロールのポリシー。

AWSResilienceHubAsssessmentExecutionPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSResilienceHubAsssessmentExecutionPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 6 月 27 日 12:32 UTC
- 編集日時: 2024 年 12 月 16 日 14:40 UTC
- ARN: arn:aws:iam::aws:policy/AWSResilienceHubAsssessmentExecutionPolicy

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSResilienceHubFullResourceStatement",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "autoscaling:DescribeAutoScalingGroups",
        "backup:DescribeBackupVault",
        "backup:GetBackupPlan",
```

```
        "backup:GetBackupSelection",
        "backup:ListBackupPlans",
        "backup:ListBackupSelections",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "cloudformation:ValidateTemplate",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "datasync:DescribeTask",
        "datasync:ListLocations",
        "datasync:ListTasks",
        "devops-guru:ListMonitoredResources",
        "dlm:GetLifecyclePolicies",
        "dlm:GetLifecyclePolicy",
        "docdb-elastic:GetCluster",
        "docdb-elastic:GetClusterSnapshot",
        "docdb-elastic:ListClusterSnapshots",
        "docdb-elastic:ListTagsForResource",
        "drs:DescribeJobs",
        "drs:DescribeSourceServers",
        "drs:GetReplicationConfiguration",
        "ds:DescribeDirectories",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeGlobalTable",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeTable",
        "dynamodb:ListGlobalTables",
        "dynamodb:ListTagsOfResource",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeFastSnapshotRestores",
        "ec2:DescribeFleets",
        "ec2:DescribeHosts",
        "ec2:DescribeInstances",
        "ec2:DescribeNatGateways",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeRegions",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcEndpoints",
        "ecr:DescribeRegistry",
        "ecs:DescribeCapacityProviders",
```

```
        "ecs:DescribeClusters",
        "ecs:DescribeContainerInstances",
        "ecs:DescribeServices",
        "ecs:DescribeTaskDefinition",
        "ecs:ListContainerInstances",
        "ecs:ListServices",
        "eks:DescribeCluster",
        "eks:DescribeFargateProfile",
        "eks:DescribeNodegroup",
        "eks:ListFargateProfiles",
        "eks:ListNodegroups",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeGlobalReplicationGroups",
        "elasticache:DescribeReplicationGroups",
        "elasticache:DescribeSnapshots",
        "elasticache:DescribeServerlessCaches",
        "elasticache:DescribeServerlessCacheSnapshots",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeReplicationConfigurations",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "fis:GetExperiment",
        "fis:GetExperimentTemplate",
        "fis:ListExperimentTemplates",
        "fis:ListExperiments",
        "fis:ListExperimentResolvedTargets",
        "fsx:DescribeFileSystems",
        "lambda:GetFunctionConcurrency",
        "lambda:GetFunctionConfiguration",
        "lambda:ListAliases",
        "lambda:ListEventSourceMappings",
        "lambda:ListFunctionEventInvokeConfigs",
        "lambda:ListVersionsByFunction",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstanceAutomatedBackups",
        "rds:DescribeDBInstances",
        "rds:DescribeDBProxies",
        "rds:DescribeDBProxyTargets",
        "rds:DescribeDBSnapshots",
```

```
        "rds:DescribeGlobalClusters",
        "rds:ListTagsForResource",
        "resource-groups:GetGroup",
        "resource-groups:ListGroupResources",
        "route53-recovery-control-config:ListClusters",
        "route53-recovery-control-config:ListControlPanels",
        "route53-recovery-control-config:ListRoutingControls",
        "route53-recovery-readiness:GetReadinessCheckStatus",
        "route53-recovery-readiness:GetResourceSet",
        "route53-recovery-readiness:ListReadinessChecks",
        "route53:GetHealthCheck",
        "route53:ListHealthChecks",
        "route53:ListHostedZones",
        "route53:ListResourceRecordSets",
        "route53resolver:ListResolverEndpoints",
        "route53resolver:ListResolverEndpointIpAddresses",
        "s3:ListBucket",
        "servicecatalog:GetApplication",
        "servicecatalog:ListAssociatedResources",
        "sns:GetSubscriptionAttributes",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptionsByTopic",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "ssm:DescribeAutomationExecutions",
        "states:DescribeStateMachine",
        "states:ListStateMachineVersions",
        "states:ListStateMachineAliases",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSResilienceHubApiGatewayStatement",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/usageplans"
      ]
    },
```

```
    {
      "Sid" : "AWSResilienceHubS3ArtifactStatement",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutObject",
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::aws-resilience-hub-artifacts-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AWSResilienceHubS3AccessStatement",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "s3:GetMultiRegionAccessPointRoutes",
        "s3:GetReplicationConfiguration",
        "s3:ListAllMyBuckets",
        "s3:ListMultiRegionAccessPoints"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AWSResilienceHubCloudWatchStatement",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "ResilienceHub"
        }
      }
    },
    {
      "Sid" : "AWSResilienceHubSSMStatement",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParametersByPath"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/ResilienceHub/*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSResourceAccessManagerFullAccess

説明: AWS Resource Access Manager へのフルアクセスを提供します

`AWSResourceAccessManagerFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSResourceAccessManagerFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 6 月 4 日 17:28 UTC

- 編集日時: 2019 年 6 月 4 日 17:28 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceAccessManagerFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSResourceAccessManagerReadOnlyAccess

説明: AWS Resource Access Manager への読み取り専用アクセスを提供します。

`AWSResourceAccessManagerReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSResourceAccessManagerReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 12 月 9 日 20:58 UTC
- 編集日時: 2019 年 12 月 9 日 20:58 UTC
- ARN: arn:aws:iam::aws:policy/AWSResourceAccessManagerReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する

- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSResourceAccessManagerResourceShareParticipantAccess

説明: AWS リソース共有参加者が必要とする Resource Access Manager APIs へのアクセスを提供します。

AWSResourceAccessManagerResourceShareParticipantAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSResourceAccessManagerResourceShareParticipantAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 12 月 9 日 20:41 UTC
- 編集日時: 2019 年 12 月 9 日 20:41 UTC
- ARN: arn:aws:iam::aws:policy/AWSResourceAccessManagerResourceShareParticipantAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSResourceAccessManagerServiceRolePolicy

説明: 顧客の Organizations 構造への読み取り専用 AWS Resource Access Manager アクセスを含むポリシー。ロールを自己削除するための IAM アクセス許可も含まれます。

`AWSResourceAccessManagerServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー

- 作成日時: 2018 年 11 月 14 日 19:28 UTC
- 編集日時: 2018 年 11 月 14 日 19:28 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSResourceAccessManagerServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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/*"
```

```
      ]
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSResourceExplorerFullAccess

説明: このポリシーは、Resource Explorer リソースにアクセスするための管理アクセス許可を付与し、このアクセスをサポートするために他の AWS サービスに読み取り専用アクセス許可を付与します。

`AWSResourceExplorerFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSResourceExplorerFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 11 月 7 日 20:01 UTC
- 編集日時: 2023 年 11 月 14 日 16:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceExplorerFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSResourceExplorerOrganizationsAccess

説明: このポリシーは、Resource Explorer に管理アクセス許可を付与し、このアクセスをサポートするために他の AWS サービスに読み取り専用アクセス許可を付与します。 AWS Organizations 管理者は、コンソールでマルチアカウント検索を設定および管理するために、これらのアクセス許可が必要です。

AWSResourceExplorerOrganizationsAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSResourceExplorerOrganizationsAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 11 月 14 日 17:01 UTC
- 編集日時: 2023 年 11 月 14 日 17:01 UTC
- ARN: arn:aws:iam::aws:policy/AWSResourceExplorerOrganizationsAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSResourceExplorerReadOnlyAccess

説明: このポリシーは、Resource Explorer リソースを検索して表示する読み取り専用アクセス許可を付与し、このアクセスをサポートするために他の AWS サービスに読み取り専用アクセス許可を付与します。

`AWSResourceExplorerReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSResourceExplorerReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 11 月 7 日 19:56 UTC
- 編集日時: 2023 年 11 月 14 日 16:43 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSResourceExplorerServiceRolePolicy

説明: Resource Explorer がユーザーに代わってリソースおよび CloudTrail イベントを閲覧し、検索用にリソースをインデックス付けをできるようにします。

AWSResourceExplorerServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 10 月 25 日 20:35 UTC
- 編集日時: 2025 年 12 月 16 日 20:19 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSResourceExplorerServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v22 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ResourceExplorerAccess",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:UpdateIndexType",
```

```
        "resource-explorer-2:CreateIndex",
        "resource-explorer-2:CreateView",
        "resource-explorer-2:AssociateDefaultView",
        "resource-explorer-2:DeleteIndex"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListAccounts",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListRoots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudTrailEventsAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateServiceLinkedChannel",
        "cloudtrail:GetServiceLinkedChannel"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:channel/aws-service-channel/resource-
explorer-2/*"
    },
    {
      "Sid" : "ApiGatewayAccess",
      "Effect" : "Allow",
      "Action" : "apigateway:GET",
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/restapis/*/deployments",
        "arn:aws:apigateway:*::/restapis/*/deployments/*",
        "arn:aws:apigateway:*::/restapis/*/resources",
        "arn:aws:apigateway:*::/restapis/*/resources/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*",
        "arn:aws:apigateway:*::/restapis/*/stages",
```

```
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/vpclinks",
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*/routes",
        "arn:aws:apigateway:*::/apis/*/stages",
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/apis/*/routes/*",
        "arn:aws:apigateway:*::/apis/*/stages/*",
        "arn:aws:apigateway:*::/apis/*/integrations",
        "arn:aws:apigateway:*::/apis/*/integrations/*"
      ]
    },
    {
      "Sid" : "ResourceInventoryAccess",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:ListAnalyzers",
        "acm-pca:ListCertificateAuthorities",
        "acm:ListCertificates",
        "airflow:ListEnvironments",
        "amplify:ListApps",
        "amplify:ListBranches",
        "amplify:ListDomainAssociations",
        "aoss:ListCollections",
        "app-integrations:ListApplications",
        "app-integrations:ListEventIntegrations",
        "appconfig:ListApplications",
        "appconfig:ListDeploymentStrategies",
        "appconfig:ListEnvironments",
        "appconfig:ListExtensionAssociations",
        "appflow:ListFlows",
        "appmesh:ListGatewayRoutes",
        "appmesh:ListMeshes",
        "appmesh:ListRoutes",
        "appmesh:ListVirtualGateways",
        "appmesh:ListVirtualNodes",
        "appmesh:ListVirtualRouters",
        "appmesh:ListVirtualServices",
        "apprunner:ListAutoScalingConfigurations",
        "apprunner:ListConnections",
        "apprunner:ListServices",
        "apprunner:ListVpcConnectors",
        "appstream:DescribeAppBlocks",
        "appstream:DescribeApplications",
```

```
        "appstream:DescribeFleets",
        "appstream:DescribeImageBuilders",
        "appstream:DescribeStacks",
        "appsync:ListGraphqlApis",
        "aps:ListRuleGroupsNamespaces",
        "aps:ListWorkspaces",
        "athena:ListDataCatalogs",
        "athena:ListWorkGroups",
        "auditmanager:GetAccountStatus",
        "auditmanager:ListAssessments",
        "autoscaling:DescribeAutoScalingGroups",
        "backup-gateway:ListHypervisors",
        "backup:ListBackupPlans",
        "backup:ListBackupVaults",
        "backup:ListReportPlans",
        "batch:DescribeComputeEnvironments",
        "batch:DescribeJobDefinitions",
        "batch:DescribeJobQueues",
        "batch:ListSchedulingPolicies",
        "bedrock:ListAgentAliases",
        "bedrock:ListAgents",
        "bedrock:ListDataAutomationProjects",
        "bedrock:ListFlows",
        "bedrock:ListGuardrails",
        "bedrock:ListInferenceProfiles",
        "bedrock:ListKnowledgeBases",
        "bedrock:ListPromptRouters",
        "bedrock:ListPrompts",
        "ce:GetAnomalyMonitors",
        "ce:GetAnomalySubscriptions",
        "chime:ListAppInstanceBots",
        "chime:ListAppInstanceUsers",
        "chime:ListAppInstances",
        "chime:ListMediaInsightsPipelineConfigurations",
        "chime:ListMediaPipelineKinesisVideoStreamPools",
        "chime:ListMediaPipelines",
        "chime:ListSipMediaApplications",
        "chime:ListVoiceConnectors",
        "cloud9:ListEnvironments",
        "cloudformation:ListResources",
        "cloudformation:ListStackSets",
        "cloudformation:ListStacks",
        "cloudfront:ListCachePolicies",
        "cloudfront:ListCloudFrontOriginAccessIdentities",
```

```
        "cloudfront:ListContinuousDeploymentPolicies",
        "cloudfront:ListDistributions",
        "cloudfront:ListFieldLevelEncryptionConfigs",
        "cloudfront:ListFieldLevelEncryptionProfiles",
        "cloudfront:ListFunctions",
        "cloudfront:ListOriginAccessControls",
        "cloudfront:ListOriginRequestPolicies",
        "cloudfront:ListRealtimeLogConfigs",
        "cloudfront:ListResponseHeadersPolicies",
        "cloudtrail:ListChannels",
        "cloudtrail:ListDashboards",
        "cloudtrail:ListEventDataStores",
        "cloudtrail:ListTrails",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeInsightRules",
        "cloudwatch:ListDashboards",
        "cloudwatch:ListMetricStreams",
        "codeartifact:ListDomains",
        "codeartifact:ListRepositories",
        "codebuild:ListProjects",
        "codecommit:ListRepositories",
        "codeconnections:ListConnections",
        "codedeploy:ListApplications",
        "codedeploy:ListDeploymentConfigs",
        "codeguru-profiler:ListProfilingGroups",
        "codeguru-reviewer:ListRepositoryAssociations",
        "codepipeline:ListPipelines",
        "codepipeline:ListWebhooks",
        "codestar-connections:ListConnections",
        "cognito-identity:ListIdentityPools",
        "cognito-idp:ListUserPools",
        "comprehend:ListDocumentClassifiers",
        "comprehend:ListEntityRecognizers",
        "comprehend:ListFlywheels",
        "config:DescribeConfigRules",
        "connect:ListEvaluationForms",
        "connect:ListHoursOfOperations",
        "connect:ListInstanceAttributes",
        "connect:ListInstances",
        "connect:ListPhoneNumbersV2",
        "connect:ListPrompts",
        "connect:ListQuickConnects",
        "connect:ListRoutingProfileQueues",
        "connect:ListRoutingProfiles",
```

```
        "connect:ListRules",
        "connect:ListSecurityProfiles",
        "connect:ListTaskTemplates",
        "connect:ListUsers",
        "databrew:ListDatasets",
        "databrew:ListJobs",
        "databrew:ListProjects",
        "databrew:ListRecipes",
        "databrew:ListRulesets",
        "databrew:ListSchedules",
        "dataexchange:ListDataSets",
        "datapipeline:ListPipelines",
        "datasync:ListLocations",
        "datasync:ListTasks",
        "dax:DescribeClusters",
        "detective:ListGraphs",
        "devicefarm:ListInstanceProfiles",
        "devicefarm:ListProjects",
        "devicefarm:ListTestGridProjects",
        "directconnect:DescribeDirectConnectGateways",
        "dms:DescribeCertificates",
        "dms:DescribeEndpoints",
        "dms:DescribeEventSubscriptions",
        "dms:DescribeReplicationInstances",
        "dms:DescribeReplicationSubnetGroups",
        "dms:DescribeReplicationTasks",
        "ds:DescribeDirectories",
        "dynamodb:ListTables",
        "ec2:DescribeAddresses",
        "ec2:DescribeCapacityReservationFleets",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeCarrierGateways",
        "ec2:DescribeClientVpnEndpoints",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeFleets",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeFpgaImages",
        "ec2:DescribeHostReservations",
        "ec2:DescribeHosts",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceConnectEndpoints",
        "ec2:DescribeInstanceEventWindows",
```

```
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeIpamPools",
        "ec2:DescribeIpamResourceDiscoveries",
        "ec2:DescribeIpamResourceDiscoveryAssociations",
        "ec2:DescribeIpamScopes",
        "ec2:DescribeIpams",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInsightsAccessScopeAnalyses",
        "ec2:DescribeNetworkInsightsAccessScopes",
        "ec2:DescribeNetworkInsightsAnalyses",
        "ec2:DescribeNetworkInsightsPaths",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePlacementGroups",
        "ec2:DescribePublicIpv4Pools",
        "ec2:DescribeReservedInstances",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSpotFleetRequests",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSubnets",
        "ec2:DescribeTrafficMirrorFilters",
        "ec2:DescribeTrafficMirrorSessions",
        "ec2:DescribeTrafficMirrorTargets",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayConnectPeers",
        "ec2:DescribeTransitGatewayMulticastDomains",
        "ec2:DescribeTransitGatewayPolicyTables",
        "ec2:DescribeTransitGatewayRouteTableAnnouncements",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeVerifiedAccessEndpoints",
        "ec2:DescribeVerifiedAccessGroups",
        "ec2:DescribeVerifiedAccessInstances",
        "ec2:DescribeVerifiedAccessTrustProviders",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcBlockPublicAccessExclusions",
        "ec2:DescribeVpcEndpointServiceConfigurations",
```

```
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetSubnetCidrReservations",
        "ecr-public:DescribeRepositories",
        "ecr:DescribeRepositories",
        "ecs:DescribeCapacityProviders",
        "ecs:DescribeServices",
        "ecs:ListClusters",
        "ecs:ListContainerInstances",
        "ecs:ListServices",
        "ecs:ListTaskDefinitions",
        "eks:DescribeAccessEntry",
        "eks:DescribeAddon",
        "eks:DescribeFargateProfile",
        "eks:DescribeIdentityProviderConfig",
        "eks:DescribeNodegroup",
        "eks:ListAccessEntries",
        "eks:ListAddons",
        "eks:ListClusters",
        "eks:ListEksAnywhereSubscriptions",
        "eks:ListFargateProfiles",
        "eks:ListIdentityProviderConfigs",
        "eks:ListNodegroups",
        "eks:ListPodIdentityAssociations",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeCacheParameterGroups",
        "elasticache:DescribeCacheSubnetGroups",
        "elasticache:DescribeGlobalReplicationGroups",
        "elasticache:DescribeReplicationGroups",
        "elasticache:DescribeReservedCacheNodes",
        "elasticache:DescribeSnapshots",
        "elasticache:DescribeUserGroups",
        "elasticache:DescribeUsers",
        "elasticbeanstalk:DescribeApplicationVersions",
        "elasticbeanstalk:DescribeApplications",
        "elasticbeanstalk:DescribeEnvironments",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeFileSystems",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
```

```
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticmapreduce:ListClusters",
        "emr-containers:ListJobTemplates",
        "emr-containers:ListManagedEndpoints",
        "emr-containers:ListSecurityConfigurations",
        "emr-containers:ListVirtualClusters",
        "emr-serverless:ListApplications",
        "es:ListDomainNames",
        "events:ListApiDestinations",
        "events:ListArchives",
        "events:ListConnections",
        "events:ListEndpoints",
        "events:ListEventBuses",
        "events:ListRules",
        "evidently:ListExperiments",
        "evidently:ListFeatures",
        "evidently:ListLaunches",
        "evidently:ListProjects",
        "finspace:ListEnvironments",
        "firehose:ListDeliveryStreams",
        "fis:ListExperimentTemplates",
        "fms:ListPolicies",
        "fms:ListProtocolsLists",
        "forecast:ListDatasetGroups",
        "forecast:ListDatasetImportJobs",
        "forecast:ListDatasets",
        "forecast:ListForecastExportJobs",
        "forecast:ListForecasts",
        "forecast:ListPredictorBacktestExportJobs",
        "forecast:ListPredictors",
        "frauddetector:GetDetectors",
        "frauddetector:GetEntityTypes",
        "frauddetector:GetEventTypes",
        "frauddetector:GetExternalModels",
        "frauddetector:GetLabels",
        "frauddetector:GetModels",
        "frauddetector:GetOutcomes",
        "frauddetector:GetVariables",
        "fsx:DescribeBackups",
        "fsx:DescribeFileSystems",
        "gamelift:DescribeGameSessionQueues",
        "gamelift:DescribeMatchmakingConfigurations",
        "gamelift:DescribeMatchmakingRuleSets",
        "gamelift:ListAliases",
```

```
        "gamelift:ListBuilds",
        "gamelift:ListLocations",
        "gamelift:ListScripts",
        "geo:ListMaps",
        "geo:ListPlaceIndexes",
        "geo:ListTrackers",
        "glacier:ListVaults",
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListEndpointGroups",
        "globalaccelerator:ListListeners",
        "glue:GetCrawlers",
        "glue:GetDatabases",
        "glue:GetJobs",
        "glue:GetTables",
        "glue:GetTriggers",
        "glue:ListDataQualityRulesets",
        "glue:ListMLTransforms",
        "glue:ListRegistries",
        "grafana:ListWorkspaces",
        "greengrass:ListComponentVersions",
        "greengrass:ListComponents",
        "greengrass:ListConnectorDefinitions",
        "greengrass:ListCoreDefinitions",
        "greengrass:ListDeviceDefinitions",
        "greengrass:ListFunctionDefinitions",
        "greengrass:ListGroups",
        "greengrass:ListLoggerDefinitions",
        "greengrass:ListResourceDefinitions",
        "greengrass:ListSubscriptionDefinitions",
        "groundstation:ListConfigs",
        "groundstation:ListDataflowEndpointGroups",
        "groundstation:ListMissionProfiles",
        "guardduty:ListDetectors",
        "guardduty:ListFilters",
        "guardduty:ListIPSets",
        "guardduty:ListMalwareProtectionPlans",
        "guardduty:ListPublishingDestinations",
        "guardduty:ListThreatIntelSets",
        "healthlake:ListFHIRDatastores",
        "iam:ListGroups",
        "iam:ListInstanceProfiles",
        "iam:ListOpenIDConnectProviders",
        "iam:ListPolicies",
        "iam:ListRoles",
```

```
        "iam:ListSAMLProviders",
        "iam:ListServerCertificates",
        "iam:ListUsers",
        "iam:ListVirtualMFADevices",
        "imagebuilder:ListComponentBuildVersions",
        "imagebuilder:ListComponents",
        "imagebuilder:ListContainerRecipes",
        "imagebuilder:ListDistributionConfigurations",
        "imagebuilder:ListImageBuildVersions",
        "imagebuilder:ListImagePipelines",
        "imagebuilder:ListImageRecipes",
        "imagebuilder:ListImages",
        "imagebuilder:ListInfrastructureConfigurations",
        "inspector2:ListFilters",
        "inspector:ListAssessmentTemplates",
        "iot:ListAuthorizers",
        "iot:ListBillingGroups",
        "iot:ListCACertificates",
        "iot:ListCertificates",
        "iot:ListFleetMetrics",
        "iot:ListJobTemplates",
        "iot:ListMitigationActions",
        "iot:ListPolicies",
        "iot:ListProvisioningTemplates",
        "iot:ListRoleAliases",
        "iot:ListScheduledAudits",
        "iot:ListSecurityProfiles",
        "iot:ListThingGroups",
        "iot:ListThingTypes",
        "iot:ListThings",
        "iot:ListTopicRuleDestinations",
        "iot:ListTopicRules",
        "iotanalytics:ListChannels",
        "iotanalytics:ListDatasets",
        "iotanalytics:ListDatastores",
        "iotanalytics:ListPipelines",
        "iotdeviceadvisor:ListSuiteDefinitions",
        "iotevents:ListAlarmModels",
        "iotevents:ListDetectorModels",
        "iotevents:ListInputs",
        "iotfleethub:ListApplications",
        "iotfleetwise:ListDecoderManifests",
        "iotfleetwise:ListModelManifests",
        "iotfleetwise:ListSignalCatalogs",
```

```
        "iotfleetwise:ListVehicles",
        "iotsitewise:ListAccessPolicies",
        "iotsitewise:ListAssetModels",
        "iotsitewise:ListAssets",
        "iotsitewise:ListDashboards",
        "iotsitewise:ListGateways",
        "iotsitewise:ListPortals",
        "iotsitewise:ListProjects",
        "iottwinmaker:ListComponentTypes",
        "iottwinmaker:ListEntities",
        "iottwinmaker:ListSyncJobs",
        "iottwinmaker:ListWorkspaces",
        "iotwireless:ListDestinations",
        "iotwireless:ListDeviceProfiles",
        "iotwireless:ListFuotaTasks",
        "iotwireless:ListMulticastGroups",
        "iotwireless:ListPartnerAccounts",
        "iotwireless:ListServiceProfiles",
        "iotwireless:ListWirelessDevices",
        "iotwireless:ListWirelessGatewayTaskDefinitions",
        "iotwireless:ListWirelessGateways",
        "ivs:ListChannels",
        "ivs:ListEncoderConfigurations",
        "ivs:ListIngestConfigurations",
        "ivs:ListPlaybackKeyPairs",
        "ivs:ListPlaybackRestrictionPolicies",
        "ivs:ListRecordingConfigurations",
        "ivs:ListStorageConfigurations",
        "ivs:ListStreamKeys",
        "ivschat:ListLoggingConfigurations",
        "ivschat:ListRooms",
        "kafka:ListClusters",
        "kafka:ListConfigurations",
        "kendra:ListAccessControlConfigurations",
        "kendra:ListDataSources",
        "kendra:ListExperiences",
        "kendra:ListFaqs",
        "kendra:ListFeaturedResultsSets",
        "kendra:ListIndices",
        "kendra:ListQuerySuggestionsBlockLists",
        "kendra:ListThesauri",
        "kinesis:ListStreams",
        "kinesisanalytics:ListApplications",
        "kinesisvideo:ListSignalingChannels",
```

```
        "kinesisvideo:ListStreams",
        "kms:ListKeys",
        "lambda:ListCodeSigningConfigs",
        "lambda:ListEventSourceMappings",
        "lambda:ListFunctions",
        "lex:ListBotAliases",
        "lex:ListBots",
        "license-manager:ListDistributedGrants",
        "lightsail:GetBuckets",
        "lightsail:GetCertificates",
        "lightsail:GetContainerServices",
        "lightsail:GetDisks",
        "logs:DescribeDestinations",
        "logs:DescribeLogGroups",
        "logs:ListTagsForResource",
        "lookoutmetrics:ListAlerts",
        "lookoutmetrics:ListAnomalyDetectors",
        "lookoutvision:ListProjects",
        "m2:ListEnvironments",
        "macie2:ListAllowLists",
        "macie2:ListCustomDataIdentifiers",
        "macie2:ListFindingsFilters",
        "managedblockchain:ListAccessors",
        "mediapackage-vod:ListAssets",
        "mediapackage-vod:ListPackagingConfigurations",
        "mediapackage-vod:ListPackagingGroups",
        "mediapackage:ListChannels",
        "mediapackage:ListOriginEndpoints",
        "mediastore:ListContainers",
        "mediatailor:ListChannels",
        "mediatailor:ListLiveSources",
        "mediatailor:ListPlaybackConfigurations",
        "mediatailor:ListSourceLocations",
        "mediatailor:ListVodSources",
        "memorydb:DescribeACLs",
        "memorydb:DescribeClusters",
        "memorydb:DescribeParameterGroups",
        "memorydb:DescribeSnapshots",
        "memorydb:DescribeSubnetGroups",
        "memorydb:DescribeUsers",
        "mobiletargeting:GetApps",
        "mobiletargeting:GetCampaigns",
        "mobiletargeting:GetSegments",
        "mobiletargeting:ListTemplates",
```

```
        "mq:ListBrokers",
        "mq:ListConfigurations",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups",
        "networkmanager:DescribeGlobalNetworks",
        "networkmanager:GetDevices",
        "networkmanager:GetLinks",
        "networkmanager:ListAttachments",
        "networkmanager:ListCoreNetworks",
        "oam:ListSinks",
        "omics:ListReferenceStores",
        "omics:ListRunGroups",
        "omics:ListWorkflows",
        "outposts:ListSites",
        "organizations:DescribeResourcePolicy",
        "organizations:ListPolicies",
        "panorama:ListPackages",
        "partnercentral:ListEngagementInvitations",
        "partnercentral:ListEngagements",
        "partnercentral:ListOpportunities",
        "partnercentral:ListResourceSnapshotJobs",
        "partnercentral:ListResourceSnapshots",
        "personalize:ListDatasetGroups",
        "personalize:ListDatasets",
        "personalize:ListSchemas",
        "personalize:ListSolutions",
        "pipes:ListPipes",
        "profile:ListDomains",
        "profile:ListIntegrations",
        "profile:ListProfileObjectTypes",
        "proton:ListEnvironmentAccountConnections",
        "proton:ListEnvironmentTemplates",
        "proton:ListServiceTemplates",
        "qldb:ListJournalKinesisStreamsForLedger",
        "qldb:ListLedgers",
        "quicksight:DescribeAccountSubscription",
        "quicksight:ListDataSets",
        "quicksight:ListDataSources",
        "quicksight:ListTemplates",
        "quicksight:ListThemes",
        "ram:GetResourceShares",
        "rds:DescribeBlueGreenDeployments",
        "rds:DescribeDBClusterEndpoints",
```

```
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstanceAutomatedBackups",
        "rds:DescribeDBInstances",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBProxies",
        "rds:DescribeDBProxyEndpoints",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBSnapshots",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeGlobalClusters",
        "rds:DescribeOptionGroups",
        "rds:DescribeReservedDBInstances",
        "redshift:DescribeClusterParameterGroups",
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeClusterSubnetGroups",
        "redshift:DescribeClusters",
        "redshift:DescribeEventSubscriptions",
        "redshift:DescribeHsmClientCertificates",
        "redshift:DescribeSnapshotCopyGrants",
        "redshift:DescribeSnapshotSchedules",
        "redshift:DescribeUsageLimits",
        "refactor-spaces:ListApplications",
        "refactor-spaces:ListEnvironments",
        "refactor-spaces:ListRoutes",
        "refactor-spaces:ListServices",
        "rekognition:DescribeProjects",
        "resiliencehub:ListApps",
        "resiliencehub:ListResiliencyPolicies",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:ListViews",
        "resource-groups:ListGroups",
        "route53-recovery-control-config:ListClusters",
        "route53-recovery-control-config:ListControlPanels",
        "route53-recovery-control-config:ListRoutingControls",
        "route53-recovery-control-config:ListSafetyRules",
        "route53-recovery-readiness:ListCells",
        "route53-recovery-readiness:ListReadinessChecks",
        "route53-recovery-readiness:ListRecoveryGroups",
        "route53-recovery-readiness:ListResourceSets",
        "route53:ListHealthChecks",
```

```
        "route53:ListHostedZones",
        "route53domains:ListDomains",
        "route53resolver:ListFirewallDomainLists",
        "route53resolver:ListFirewallRuleGroupAssociations",
        "route53resolver:ListFirewallRuleGroups",
        "route53resolver:ListResolverEndpoints",
        "route53resolver:ListResolverQueryLogConfigs",
        "route53resolver:ListResolverRules",
        "rum:ListAppMonitors",
        "s3:GetBucketLocation",
        "s3:ListAccessPoints",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListMultiRegionAccessPoints",
        "s3:ListStorageLensConfigurations",
        "s3:ListStorageLensGroups",
        "s3express:ListAllMyDirectoryBuckets",
        "sagemaker:ListActions",
        "sagemaker:ListAlgorithms",
        "sagemaker:ListAppImageConfigs",
        "sagemaker:ListApps",
        "sagemaker:ListArtifacts",
        "sagemaker:ListClusters",
        "sagemaker:ListCodeRepositories",
        "sagemaker:ListContexts",
        "sagemaker:ListDomains",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListEndpoints",
        "sagemaker:ListExperiments",
        "sagemaker:ListFeatureGroups",
        "sagemaker:ListFlowDefinitions",
        "sagemaker:ListHubContents",
        "sagemaker:ListHubs",
        "sagemaker:ListHumanTaskUis",
        "sagemaker:ListImageVersions",
        "sagemaker:ListImages",
        "sagemaker:ListInferenceComponents",
        "sagemaker:ListInferenceExperiments",
        "sagemaker:ListMlflowTrackingServers",
        "sagemaker:ListModelCardVersions",
        "sagemaker:ListModelCards",
        "sagemaker:ListModelPackageGroups",
        "sagemaker:ListModelPackages",
        "sagemaker:ListModels",
```

```
        "sagemaker:ListMonitoringSchedules",
        "sagemaker:ListNotebookInstanceLifecycleConfigs",
        "sagemaker:ListNotebookInstances",
        "sagemaker:ListPipelines",
        "sagemaker:ListProjects",
        "sagemaker:ListSpaces",
        "sagemaker:ListStudioLifecycleConfigs",
        "sagemaker:ListTrialComponents",
        "sagemaker:ListTrials",
        "sagemaker:ListUserProfiles",
        "sagemaker:ListWorkforces",
        "sagemaker:ListWorkteams",
        "scheduler:ListScheduleGroups",
        "schemas:ListDiscoverers",
        "secretsmanager:ListSecrets",
        "servicecatalog:ListApplications",
        "servicecatalog:ListAttributeGroups",
        "servicediscovery:ListServices",
        "ses:ListConfigurationSets",
        "ses:ListContactLists",
        "ses:ListDedicatedIpPools",
        "ses:ListEmailIdentities",
        "shield:ListProtectionGroups",
        "shield:ListProtections",
        "signer:ListSigningProfiles",
        "sns:ListTopics",
        "sqs:ListQueues",
        "ssm-incidents:ListResponsePlans",
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeMaintenanceWindowTargets",
        "ssm:DescribeMaintenanceWindowTasks",
        "ssm:DescribeMaintenanceWindows",
        "ssm:DescribeParameters",
        "ssm:DescribeSessions",
        "ssm:ListAssociations",
        "ssm:ListDocuments",
        "ssm:ListResourceDataSync",
        "states:ListActivities",
        "states:ListStateMachines",
        "storagegateway:ListGateways",
        "synthetics:DescribeCanaries",
        "synthetics:ListGroups",
        "transfer:ListAgreements",
        "transfer:ListCertificates",
```

```
        "transfer:ListConnectors",
        "transfer:ListProfiles",
        "transfer:ListServers",
        "transfer:ListUsers",
        "transfer:ListWorkflows",
        "verifiedpermissions:ListPolicyStores",
        "vpc-lattice:ListListeners",
        "vpc-lattice:ListServiceNetworkServiceAssociations",
        "vpc-lattice:ListServiceNetworks",
        "vpc-lattice:ListServices",
        "vpc-lattice:ListTargetGroups",
        "wafv2:ListIPSets",
        "wafv2:ListRegexPatternSets",
        "wafv2:ListRuleGroups",
        "wafv2:ListWebACLs",
        "wisdom:ListAssistantAssociations",
        "wisdom:ListAssistants",
        "wisdom:ListContents",
        "wisdom:ListKnowledgeBases",
        "workspaces-web:ListPortals",
        "workspaces:DescribeConnectionAliases",
        "workspaces:DescribeWorkspaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PermissionsForReadGetResources",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetAgent",
        "bedrock:GetAgentActionGroup",
        "bedrock:GetAgentCollaborator",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:GetGuardrail",
        "bedrock:GetKnowledgeBase",
        "bedrock:ListAgentActionGroups",
        "bedrock:ListAgentCollaborators",
        "bedrock:ListAgentKnowledgeBases",
        "bedrock:ListTagsForResource",
        "cloudformation:GetResource",
        "cloudfront:GetDistribution",
        "cloudfront:GetDistributionConfig",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeContributorInsights",
```

```
        "dynamodb:DescribeKinesisStreamingDestination",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:GetResourcePolicy",
        "dynamodb:ListTagsOfResource",
        "ecs:DescribeClusters",
        "ecs:DescribeTaskDefinition",
        "ecs:ListTagsForResource",
        "eks:DescribeCluster",
        "elasticloadbalancing:DescribeCapacityReservation",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancerPolicies",
        "elasticloadbalancing:DescribeLoadBalancerPolicyTypes",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetHealth",
        "events:DescribeRule",
        "events:ListTagsForResource",
        "events:ListTargetsByRule",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "kinesis:DescribeStreamSummary",
        "kinesis:ListTagsForStream",
        "lambda:GetEventSourceMapping",
        "lambda:GetFunction",
        "lambda:GetFunctionCodeSigningConfig",
        "lambda:GetFunctionRecursionConfig",
        "lambda:GetRuntimeManagementConfig",
        "lambda:ListTags",
        "logs:DescribeIndexPolicies",
        "logs:DescribeResourcePolicies",
        "logs:GetDataProtectionPolicy",
        "route53:GetHostedZone",
        "route53:ListQueryLoggingConfigs",
        "route53:ListTagsForResource",
        "s3:GetAccelerateConfiguration",
        "s3:GetAnalyticsConfiguration",
        "s3:GetBucketCORS",
        "s3:GetBucketLogging",
        "s3:GetBucketMetadataTableConfiguration",
```

```
        "s3:GetBucketNotification",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketOwnershipControls",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "s3:GetBucketWebsite",
        "s3:GetEncryptionConfiguration",
        "s3:GetIntelligentTieringConfiguration",
        "s3:GetInventoryConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetMetricsConfiguration",
        "s3:GetReplicationConfiguration",
        "sagemaker:DescribeEndpoint",
        "sagemaker:ListTags",
        "sns:GetDataProtectionPolicy",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTagsForResource",
        "sqs:GetQueueAttributes",
        "sqs:ListQueueTags"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSResourceGroupsReadOnlyAccess

説明: これは AWS Resource Groups の読み取り専用ポリシーです

`AWSResourceGroupsReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSResourceGroupsReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 3 月 7 日 10:27 UTC
- 編集日時: 2019 年 2 月 5 日 17:56 UTC
- ARN: arn:aws:iam::aws:policy/AWSResourceGroupsReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSRoboMaker_FullAccess

説明: AWS マネジメントコンソール および SDK 経由で AWS RoboMaker へのフルアクセスを提供します。関連サービス (S3 や IAM など) への限定アクセスも提供します。

AWSRoboMaker_FullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSRoboMaker_FullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 9 月 10 日 18:34 UTC
- 編集日時: 2021 年 9 月 16 日 21:06 UTC
- ARN: arn:aws:iam::aws:policy/AWSRoboMaker_FullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSRoboMakerReadOnlyAccess

説明: AWS マネジメントコンソール および SDK 経由で AWS RoboMaker への読み取り専用アクセスを提供します

`AWSRoboMakerReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSRoboMakerReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 11 月 26 日 05:30 UTC
- 編集日時: 2020 年 8 月 28 日 23:10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRoboMakerReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : [
        "robomaker:List*",
        "robomaker:BatchDescribe*",
        "robomaker:Describe*",
        "robomaker:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSRoboMakerServicePolicy

説明: RoboMaker サービスポリシー

AWSRoboMakerServicePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 11 月 26 日 06:30 UTC

- 編集日時: 2021 年 11 月 11 日 22:23 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSRoboMakerServicePolicy

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSRoboMakerServiceRolePolicy

説明: RoboMaker サービスポリシー

AWSRoboMakerServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSRoboMakerServiceRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 11 月 26 日 05:33 UTC
- 編集日時: 2018 年 11 月 26 日 05:33 UTC
- ARN: arn:aws:iam::aws:policy/AWSRoboMakerServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSRolesAnywhereFullAccess

説明: CreateProfile、DeleteTrustAnchor、DisableCRL、ResetNotificationSettings など、IAM Roles Anywhere リソースに対するすべてのアクセス許可を提供します。

AWSRolesAnywhereFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSRolesAnywhereFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 7 月 16 日 14:52 UTC
- 編集日時: 2025 年 7 月 16 日 14:52 UTC
- ARN: arn:aws:iam::aws:policy/AWSRolesAnywhereFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TrustAnchors",
      "Effect" : "Allow",
      "Action" : [
        "rolesanywhere:ListTrustAnchors",
        "rolesanywhere:GetTrustAnchor",
        "rolesanywhere:CreateTrustAnchor",
        "rolesanywhere:DeleteTrustAnchor",
        "rolesanywhere:DisableTrustAnchor",
```

```
        "rolesanywhere:EnableTrustAnchor",
        "rolesanywhere:UpdateTrustAnchor"
      ],
      "Resource" : [
        "arn:aws:rolesanywhere:*:*:trust-anchor/*"
      ]
    },
    {
      "Sid" : "Profiles",
      "Effect" : "Allow",
      "Action" : [
        "rolesanywhere:ListProfiles",
        "rolesanywhere:GetProfile",
        "rolesanywhere:CreateProfile",
        "rolesanywhere:DeleteProfile",
        "rolesanywhere:DisableProfile",
        "rolesanywhere:EnableProfile",
        "rolesanywhere:UpdateProfile"
      ],
      "Resource" : [
        "arn:aws:rolesanywhere:*:*:profile/*"
      ]
    },
    {
      "Sid" : "CRLs",
      "Effect" : "Allow",
      "Action" : [
        "rolesanywhere:ListCrls",
        "rolesanywhere:GetCrl",
        "rolesanywhere:DeleteCrl",
        "rolesanywhere:DisableCrl",
        "rolesanywhere:EnableCrl",
        "rolesanywhere:ImportCrl",
        "rolesanywhere:UpdateCrl"
      ],
      "Resource" : [
        "arn:aws:rolesanywhere:*:*:crl/*"
      ]
    },
    {
      "Sid" : "Subjects",
      "Effect" : "Allow",
      "Action" : [
        "rolesanywhere:ListSubjects",
```

```
        "rolesanywhere:GetSubject"
      ],
      "Resource" : [
        "arn:aws:rolesanywhere:*:*:subject/*"
      ]
    },
    {
      "Sid" : "OtherRolesAnywherePermissions",
      "Effect" : "Allow",
      "Action" : [
        "rolesanywhere:PutAttributeMapping",
        "rolesanywhere:DeleteAttributeMapping",
        "rolesanywhere:ResetNotificationSettings",
        "rolesanywhere:ListTagsForResource",
        "rolesanywhere:TagResource",
        "rolesanywhere:UntagResource",
        "rolesanywhere:PutNotificationSettings"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassRoleToRolesAnywhere",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "rolesanywhere.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CreateRolesAnywhereServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "rolesanywhere.amazonaws.com"
        }
      }
    }
  ]
```

```
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSRolesAnywhereReadOnly

説明: GetTrustAnchor、ListProfiles、GetCRL など、IAM Roles Anywhere リソースへの読み取り専用アクセス許可を提供します。このポリシーには、他のサービスに対する他のアクセス許可は含まれません。

`AWSRolesAnywhereReadOnly` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSRolesAnywhereReadOnly` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 7 月 16 日 15:07 UTC
- 編集日時: 2025 年 7 月 16 日 15:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRolesAnywhereReadOnly`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Profiles",
      "Effect" : "Allow",
      "Action" : [
        "rolesanywhere:ListProfiles",
        "rolesanywhere:GetProfile"
      ],
      "Resource" : [
        "arn:aws:rolesanywhere:*:*:profile/*"
      ]
    },
    {
      "Sid" : "CRLs",
      "Effect" : "Allow",
      "Action" : [
        "rolesanywhere:ListCrls",
        "rolesanywhere:GetCrl"
      ],
      "Resource" : [
        "arn:aws:rolesanywhere:*:*:crl/*"
      ]
    },
    {
      "Sid" : "Subjects",
      "Effect" : "Allow",
      "Action" : [
        "rolesanywhere:ListSubjects",
        "rolesanywhere:GetSubject"
      ],
      "Resource" : [
        "arn:aws:rolesanywhere:*:*:subject/*"
      ]
    },
    {
      "Sid" : "TrustAnchors",
      "Effect" : "Allow",
      "Action" : [
        "rolesanywhere:ListTrustAnchors",
```

```
        "rolesanywhere:GetTrustAnchor"
      ],
      "Resource" : [
        "arn:aws:rolesanywhere:*:*:trust-anchor/*"
      ]
    },
    {
      "Sid" : "Tags",
      "Effect" : "Allow",
      "Action" : [
        "rolesanywhere:ListTagsForResource"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSRolesAnywhereServicePolicy

説明: IAM Roles Anywhere がユーザーに代わって CloudWatch にサービス/使用状況のメトリクスを公開し、Private Certificate Authorities のステータスを確認できるようにします。

`AWSRolesAnywhereServicePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 7 月 5 日 15:26 UTC
- 編集日時: 2022 年 7 月 5 日 15:26 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSRolesAnywhereServicePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSS3OnOutpostsServiceRolePolicy

説明: Amazon S3 on Outposts サービスがユーザーに代わって EC2 ネットワークリソースを管理できるようにします。

AWSS3OnOutpostsServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 10 月 3 日 20:32 UTC
- 編集日時: 2023 年 10 月 3 日 20:32 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSS3OnOutpostsServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSSavingsPlansFullAccess

説明: Savings Plans サービスへのフルアクセスを提供します

`AWSSavingsPlansFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSSavingsPlansFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 11 月 6 日 22:45 UTC
- 編集日時: 2019 年 11 月 6 日 22:45 UTC
- ARN: arn:aws:iam::aws:policy/AWSSavingsPlansFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSSavingsPlansReadOnlyAccess

説明: Savings Plans サービスへの読み取り専用アクセスを提供します

AWSSavingsPlansReadOnlyAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSSavingsPlansReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 11 月 6 日 22:45 UTC
- 編集日時: 2019 年 11 月 6 日 22:45 UTC
- ARN: arn:aws:iam::aws:policy/AWSSavingsPlansReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSSecretsManagerClientReadOnlyAccess

説明: Secrets Manager からシークレットを取得して記述するためのアクセスを提供します。このポリシーでは、Secrets Manager シークレットの KMS キーの復号も許可されます。

`AWSSecretsManagerClientReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSSecretsManagerClientReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 11 月 5 日 20:04 UTC
- 編集日時: 2025 年 11 月 5 日 20:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecretsManagerClientReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecretsManagerGetAndDescribeSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*"
    },
    {
      "Sid" : "KMSDecryptKey",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:EncryptionContext:SecretARN" : "arn:aws:secretsmanager:*:*:secret:*",
          "kms:ViaService" : "secretsmanager.*.amazonaws.com"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSSecurityHubFullAccess

説明: AWS Security Hub を使用するためのフルアクセスを提供します。

`AWSSecurityHubFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSSecurityHubFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 11 月 27 日 23:54 UTC
- 編集日時: 2025 年 11 月 21 日 21:19 UTC
- ARN: arn:aws:iam::aws:policy/AWSSecurityHubFullAccess

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecurityHubAllowAll",
      "Effect" : "Allow",
      "Action" : "securityhub:*",
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityHubServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "securityhub.amazonaws.com",
```

```
            "securityhubv2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "OtherServicePermission",
      "Effect" : "Allow",
      "Action" : [
        "guardduty:GetDetector",
        "guardduty:ListDetectors",
        "guardduty:UpdateDetector",
        "guardduty:EnableOrganizationAdminAccount",
        "guardduty:ListOrganizationAdminAccounts",
        "guardduty:DeleteDetector",
        "guardduty:CreateDetector",
        "guardduty:CreateMembers",
        "guardduty:UpdateOrganizationConfiguration",
        "guardduty:DescribeOrganizationConfiguration",
        "inspector2:BatchGetAccountStatus",
        "inspector2:Enable",
        "inspector2:Disable",
        "inspector2:EnableDelegatedAdminAccount",
        "inspector2:DisableDelegatedAdminAccount",
        "inspector2:ListDelegatedAdminAccounts",
        "inspector2:UpdateOrganizationConfiguration",
        "inspector2:DescribeOrganizationConfiguration",
        "pricing:GetProducts",
        "account:ListRegions",
        "account:GetRegionOptStatus",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSSecurityHubOrganizationsAccess

説明: 組織内の AWS Security Hub を有効化および管理するためのアクセス許可を付与します。組織全体でサービスの有効化およびサービスの委任管理者アカウントの決定が含まれます。

`AWSSecurityHubOrganizationsAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSSecurityHubOrganizationsAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 3 月 15 日 20:53 UTC
- 編集日時: 2025 年 11 月 21 日 21:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityHubOrganizationsAccess`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
      "Action" : [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:ListRoots",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAccountsForParent",
        "organizations:ListParents",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
        "organizations:ListTargetsForPolicy",
        "organizations:DescribeResourcePolicy"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationPermissionsEnable",
      "Effect" : "Allow",
      "Action" : "organizations:EnableAWSServiceAccess",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "securityhub.amazonaws.com",
            "inspector2.amazonaws.com",
            "guardduty.amazonaws.com",
            "malware-protection.guardduty.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "OrganizationPermissionsDelegatedAdmin",
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource" : "arn:aws:organizations::*:account/o-*/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "organizations:ServicePrincipal" : [
            "securityhub.amazonaws.com",
            "inspector2.amazonaws.com",
            "guardduty.amazonaws.com",
            "malware-protection.guardduty.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "OrganizationPolicyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribePolicy",
        "organizations:DescribeEffectivePolicy",
        "organizations:CreatePolicy",
        "organizations:UpdatePolicy",
        "organizations:DeletePolicy",
        "organizations:AttachPolicy",
        "organizations:DetachPolicy",
        "organizations:EnablePolicyType",
        "organizations:DisablePolicyType"
      ],
      "Resource" : [
        "arn:aws:organizations::*:root/o-*/*",
        "arn:aws:organizations::*:account/o-*/*",
        "arn:aws:organizations::*:ou/o-*/*",
        "arn:aws:organizations::*:policy/o-*/securityhub_policy/*",
        "arn:aws:organizations::*:policy/o-*/inspector_policy/*"
      ],
      "Condition" : {
        "StringLikeIfExists" : {
          "organizations:PolicyType" : [
            "SECURITYHUB_POLICY",
            "INSPECTOR_POLICY"
          ]
        }
      }
    },
    {
      "Sid" : "OrganizationPolicyTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:TagResource",
```

```
        "organizations:UntagResource",
        "organizations:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:organizations::*:policy/o-*/securityhub_policy/*",
        "arn:aws:organizations::*:policy/o-*/inspector_policy/*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSSecurityHubReadOnlyAccess

説明: AWS Security Hub リソースへの読み取り専用アクセスを提供します

`AWSSecurityHubReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSSecurityHubReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 11 月 28 日 01:34 UTC
- 編集日時: 2024 年 2 月 22 日 23:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityHubReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSSecurityHubServiceRolePolicy

説明: AWS Security Hub がリソースにアクセスするために必要なサービスにリンクされたロール。

AWSSecurityHubServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 11 月 27 日 23:47 UTC
- 編集日時: 2023 年 11 月 27 日 03:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSecurityHubServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v14 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSSecurityHubV2ServiceRolePolicy

説明: このポリシーにより、Security Hub は組織内およびユーザーに代わって AWS Config ルールと Security Hub リソースを管理できます。

`AWSSecurityHubV2ServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2025 年 6 月 10 日 17:37 UTC
- 編集日時: 2025 年 11 月 17 日 18:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSecurityHubV2ServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecurityHubV2ServiceRoleAssetsConfig",
      "Effect" : "Allow",
      "Action" : [
        "config:DeleteServiceLinkedConfigurationRecorder",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:PutServiceLinkedConfigurationRecorder"
      ],
      "Resource" : [
        "arn:aws:config:*:*:configuration-recorder/
AWSConfigurationRecorderForSecurityHubAssets/*",
        "arn:aws:config:*:*:configuration-recorder/
AWSConfigurationRecorderForSecurityHubAssetsGlobal/*"
      ]
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleAssetsIamPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/config.amazonaws.com/
AWSServiceRoleForConfig",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "config.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleSecurityHubPermissions",
      "Effect" : "Allow",
      "Action" : [
        "securityhub:DisableSecurityHubV2",
        "securityhub:EnableSecurityHubV2",
        "securityhub:DescribeSecurityHubV2"
      ],
      "Resource" : "arn:aws:securityhub:*:*:hubv2/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleOrganizationsPermissionsOnResources",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganizationalUnit"
      ],
      "Resource" : "arn:aws:organizations::*:*"
    },
    {
```

```
      "Sid" : "SecurityHubV2ServiceRoleOrganizationsPermissionsWithoutResources",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListChildren"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleDelegatedAdminPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "securityhub.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleEcrListingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecr:DescribeImages",
        "ecr:DescribeRepositories"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleLambdaMetricPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleLambdaListingPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleIamListingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "iam:GetAccountSummary"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSSecurityIncidentResponseCaseFullAccess

説明: ポリシーは、Security Incident Response サービスを通じて作成されたケースリソースに対する読み取りおよび書き込みアクセス許可を顧客に提供します。

`AWSSecurityIncidentResponseCaseFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSSecurityIncidentResponseCaseFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 12 月 1 日 23:21 UTC

- 編集日時: 2024 年 12 月 1 日 23:21 UTC
- ARN: arn:aws:iam::aws:policy/AWSSecurityIncidentResponseCaseFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecurityIRCaseReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "security-ir:GetCase",
        "security-ir:ListCases",
        "security-ir:GetCaseAttachmentDownloadUrl",
        "security-ir:ListComments",
        "security-ir:ListCaseEdits"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityIRCaseTagReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "security-ir:ListTagsForResource"
      ],
      "Resource" : "arn:aws:security-ir:*:*:case/*"
    },
    {
      "Sid" : "SecurityIRCaseWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "security-ir:CreateCase",
```

```
        "security-ir:UpdateCase",
        "security-ir:CloseCase",
        "security-ir:UpdateCaseStatus",
        "security-ir:UpdateResolverType",
        "security-ir:GetCaseAttachmentUploadUrl",
        "security-ir:CreateCaseComment",
        "security-ir:UpdateCaseComment"
      ],
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:MultiFactorAuthPresent" : "true"
        }
      }
    },
    {
      "Sid" : "SecurityIRCaseTagWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "security-ir:TagResource",
        "security-ir:UntagResource"
      ],
      "Resource" : "arn:aws:security-ir:*:*:case/*",
      "Condition" : {
        "Bool" : {
          "aws:MultiFactorAuthPresent" : "true"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSSecurityIncidentResponseFullAccess

説明: ポリシーは、Security Incident Response サービスに関連付けられたすべてのリソースに対する読み取りおよび書き込みアクセス許可を顧客に提供します。

AWSSecurityIncidentResponseFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSSecurityIncidentResponseFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 12 月 1 日 23:21 UTC
- 編集日時: 2024 年 12 月 1 日 23:21 UTC
- ARN: arn:aws:iam::aws:policy/AWSSecurityIncidentResponseFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecurityIRReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "security-ir:BatchGetMemberAccountDetails",
        "security-ir:GetMembership",
        "security-ir:ListMemberships",
        "security-ir:GetCase",
```

```
        "security-ir:ListCases",
        "security-ir:GetCaseAttachmentDownloadUrl",
        "security-ir:ListComments",
        "security-ir:ListCaseEdits",
        "security-ir:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityIRWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "security-ir:CreateMembership",
        "security-ir:UpdateMembership",
        "security-ir:CancelMembership",
        "security-ir:CreateCase",
        "security-ir:UpdateCase",
        "security-ir:CloseCase",
        "security-ir:UpdateCaseStatus",
        "security-ir:UpdateResolverType",
        "security-ir:GetCaseAttachmentUploadUrl",
        "security-ir:CreateCaseComment",
        "security-ir:UpdateCaseComment",
        "security-ir:TagResource",
        "security-ir:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:MultiFactorAuthPresent" : "true"
        }
      }
    },
    {
      "Sid" : "AllowCreationOfServiceLinkedRoleForSecurityIncidentResponse",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/security-ir.amazonaws.com/
AWSServiceRoleForSecurityIncidentResponse"
      ],
      "Condition" : {
```

```
        "StringLike" : {
          "iam:AWSServiceName" : "security-ir.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowCreationOfServiceLinkedRoleForSecurityIncidentResponseTriage",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/triage.security-ir.amazonaws.com/
AWSServiceRoleForSecurityIncidentResponse_Triage"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "triage.security-ir.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "OrganizationsPolicies",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSSecurityIncidentResponseReadOnlyAccess

説明: ポリシーは、Security Incident Response サービスに関連付けられたすべてのリソースへの読み取り専用アクセス許可を顧客に提供します。アクセス許可には、ケースアタッチメントのダウンロード URL を取得するための GetCaseAttachmentDownloadUrl へのアクセスも含まれます。

`AWSSecurityIncidentResponseReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSSecurityIncidentResponseReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 12 月 1 日 23:06 UTC
- 編集日時: 2024 年 12 月 1 日 23:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityIncidentResponseReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
        "security-ir:BatchGetMemberAccountDetails",
        "security-ir:GetMembership",
        "security-ir:ListMemberships",
        "security-ir:GetCase",
        "security-ir:ListCases",
        "security-ir:GetCaseAttachmentDownloadUrl",
        "security-ir:ListComments",
        "security-ir:ListCaseEdits",
        "security-ir:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSSecurityIncidentResponseServiceRolePolicy

説明: セキュリティインシデント対応が管理または使用する AWS リソースへのアクセスを提供します

AWSSecurityIncidentResponseServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー

- 作成日時: 2024 年 12 月 1 日 16:36 UTC
- 編集日時: 2025 年 11 月 21 日 04:34 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSSecurityIncidentResponseServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecurityIncidentResponseOrganizationsPolicy",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:ListChildren",
        "organizations:DescribeAccount",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityIncidentResponseCreateCasePolicyTagOnCreate",
      "Effect" : "Allow",
      "Action" : [
        "security-ir:TagResource",
        "security-ir:CreateCase"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SecurityIncidentResponseManaged"
          ]
```

```
        },
        "StringEquals" : {
          "aws:RequestTag/SecurityIncidentResponseManaged" : "true",
          "aws:ResourceTag/SecurityIncidentResponseManaged" : "true"
        }
      },
      "Resource" : "arn:aws:security-ir:*:*:case/*"
    },
    {
      "Sid" : "SecurityIncidentResponseOperationsPolicy",
      "Effect" : "Allow",
      "Action" : [
        "security-ir:GetCase",
        "security-ir:UpdateCase",
        "security-ir:ListCases",
        "security-ir:CreateCaseComment",
        "security-ir:ListComments"
      ],
      "Resource" : "arn:aws:security-ir:*:*:case/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSSecurityIncidentResponseTriageServiceRolePolicy

説明: AWS Security Incident Response にアクセスして、セキュリティ脅威の環境を継続的にモニタリングし、セキュリティサービスを調整してアラートノイズを減らし、情報を収集して潜在的なインシデントを調査します。

AWSSecurityIncidentResponseTriageServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2024 年 12 月 1 日 16:36 UTC
- 編集日時: 2025 年 6 月 2 日 18:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSecurityIncidentResponseTriageServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "triage.security-ir.amazonaws.com"
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "guardduty:ArchiveFindings",
        "guardduty:CreateFilter",
        "guardduty:DescribeMalwareScans",
        "guardduty:GetAdministratorAccount",
        "guardduty:GetDetector",
        "guardduty:GetFilter",
        "guardduty:GetFindings",
        "guardduty:ListDetectors",
        "guardduty:ListFilters",
        "guardduty:StartMalwareScan",
        "guardduty:UpdateFindingsFeedback"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "securityhub:BatchUpdateFindings",
        "securityhub:DescribeHub",
        "securityhub:GetEnabledStandards",
        "securityhub:GetFindings",
        "securityhub:ListEnabledProductsForImport",
        "securityhub:UpdateFindings"
      ],
      "Resource" : "arn:aws:securityhub:*:*:hub/default"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "security-ir:CreateCase",
        "security-ir:TagResource"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SecurityIncidentResponseManaged"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/SecurityIncidentResponseManaged" : "true",
          "aws:ResourceTag/SecurityIncidentResponseManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "security-ir:UpdateCase"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SecurityIncidentResponseManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "security-ir:GetMembership",
        "security-ir:ListMemberships"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSServiceCatalogAdminFullAccess

説明: サービスカタログの管理者機能へのフルアクセスを提供します

AWSServiceCatalogAdminFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSServiceCatalogAdminFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 2 月 15 日 17:19 UTC
- 編集日時: 2023 年 4 月 13 日 18:43 UTC
- ARN: arn:aws:iam::aws:policy/AWSServiceCatalogAdminFullAccess

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSServiceCatalogAdminReadOnlyAccess

説明: Service Catalog の管理者機能への読み取り専用アクセスを提供します

`AWSServiceCatalogAdminReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSServiceCatalogAdminReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 10 月 25 日 18:53 UTC
- 編集日時: 2019 年 10 月 25 日 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogAdminReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSServiceCatalogAppRegistryFullAccess

説明: Service Catalog App Registry 機能へのフルアクセスを提供します

`AWSServiceCatalogAppRegistryFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSServiceCatalogAppRegistryFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2020 年 11 月 12 日 22:25 UTC
- 編集日時: 2023 年 12 月 7 日 21:50 UTC
- ARN: arn:aws:iam::aws:policy/AWSServiceCatalogAppRegistryFullAccess

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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:*:*:*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSServiceCatalogAppRegistryReadOnlyAccess

説明: Service Catalog App Registry 機能への読み取り専用アクセスを提供します

`AWSServiceCatalogAppRegistryReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSServiceCatalogAppRegistryReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 11 月 12 日 22:34 UTC
- 編集日時: 2022 年 11 月 17 日 18:16 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogAppRegistryReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSServiceCatalogAppRegistryServiceRolePolicy

説明: Service Catalog AppRegistry がユーザーに代わって Resource Group を管理できるようにします

`AWSServiceCatalogAppRegistryServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 5 月 18 日 22:18 UTC
- 編集日時: 2022 年 10 月 26 日 16:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogAppRegistryServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSServiceCatalogEndUserFullAccess

説明: サービスカタログのエンドユーザー機能へのフルアクセスを提供します

AWSServiceCatalogEndUserFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSServiceCatalogEndUserFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 2 月 15 日 17:22 UTC
- 編集日時: 2019 年 7 月 10 日 20:30 UTC
- ARN: arn:aws:iam::aws:policy/AWSServiceCatalogEndUserFullAccess

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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"
```

```
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSServiceCatalogEndUserReadOnlyAccess

説明: Service Catalog のエンドユーザー機能への読み取り専用アクセスを提供します

`AWSServiceCatalogEndUserReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSServiceCatalogEndUserReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 10 月 25 日 18:49 UTC
- 編集日時: 2019 年 10 月 25 日 18:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogEndUserReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSServiceCatalogOrgsDataSyncServiceRolePolicy

説明: AWS Organizations 組織構造と同期するための AWS ServiceCatalog のサービスにリンクされたロールポリシー

`AWSServiceCatalogOrgsDataSyncServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 4 月 10 日 20:48 UTC
- 編集日時: 2025 年 12 月 8 日 19:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogOrgsDataSyncServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "OrganizationsDataSyncToServiceCatalog",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "OrganizationsDataSyncToServiceCatalogRegions",
      "Effect" : "Allow",
      "Action" : [
        "account:ListRegions"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSServiceCatalogSyncServiceRolePolicy

説明: ソースリポジトリからプロビジョニングアーティファクトを同期するための AWS ServiceCatalog のサービスにリンクされたロール

AWSServiceCatalogSyncServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 11 月 15 日 21:20 UTC

- 編集日時: 2024 年 5 月 3 日 17:12 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogSyncServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSServiceRoleForAmazonEKSNodegroup

説明: 顧客のアカウントでノードグループを管理するために必要なアクセス許可。これらのポリシーは、AutoscalingGroups、SecurityGroups、LaunchTemplates、InstanceProfiles のリソースの管理に関連しています。

`AWSServiceRoleForAmazonEKSNodegroup` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 11 月 7 日 01:34 UTC
- 編集日時: 2024 年 11 月 21 日 00:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForAmazonEKSNodegroup`

ポリシーのバージョン

ポリシーのバージョン: v10 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SharedSecurityGroupRelatedPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DescribeInstances",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/eks" : "*"
        }
      }
    },
    {
      "Sid" : "EKSCreatedSecurityGroupRelatedPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DescribeInstances",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/eks:nodegroup-name" : "*"
        }
      }
    },
    {
      "Sid" : "LaunchTemplateRelatedPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/eks:nodegroup-name" : "*"
        }
      }
    },
    {
      "Sid" : "AutoscalingRelatedPermissions",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:UpdateAutoScalingGroup",
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:TerminateInstanceInAutoScalingGroup",
        "autoscaling:CompleteLifecycleAction",
        "autoscaling:PutLifecycleHook",
        "autoscaling:PutNotificationConfiguration",
        "autoscaling:EnableMetricsCollection",
        "autoscaling:PutScheduledUpdateGroupAction",
        "autoscaling:ResumeProcesses",
        "autoscaling:SuspendProcesses"
      ],
      "Resource" : "arn:aws:autoscaling:*:*:*:autoScalingGroupName/eks-*"
    },
    {
      "Sid" : "AllowAutoscalingToCreateSLR",
      "Effect" : "Allow",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "autoscaling.amazonaws.com"
        }
```

```
      },
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowASGCreationByEKS",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:CreateOrUpdateTags",
        "autoscaling:CreateAutoScalingGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "eks",
            "eks:cluster-name",
            "eks:nodegroup-name"
          ]
        }
      }
    },
    {
      "Sid" : "AllowPassRoleToAutoscaling",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleToEC2",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "PermissionsToManageResourcesForNodegroups",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "ec2:CreateLaunchTemplate",
        "ec2:DescribeInstances",
        "iam:GetInstanceProfile",
        "ec2:DescribeLaunchTemplates",
        "autoscaling:DescribeAutoScalingGroups",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:RunInstances",
        "ec2:DescribeSecurityGroups",
        "ec2:GetConsoleOutput",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeCapacityReservations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PermissionsToCreateAndManageInstanceProfiles",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:AddRoleToInstanceProfile"
      ],
      "Resource" : "arn:aws:iam::*:instance-profile/eks-*"
    },
    {
      "Sid" : "PermissionsToDeleteEKSAndKubernetesTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
```

```
            "eks",
            "eks:cluster-name",
            "eks:nodegroup-name",
            "kubernetes.io/cluster/*"
          ]
        }
      }
    },
    {
      "Sid" : "PermissionsForManagedNodegroupsAutoRepair",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RebootInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/eks:nodegroup-name" : "*"
        }
      }
    },
    {
      "Sid" : "PermissionsToCreateEKSAndKubernetesTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:*:ec2:*:*:security-group/*",
        "arn:*:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "eks",
            "eks:cluster-name",
            "eks:nodegroup-name",
            "kubernetes.io/cluster/*"
          ]
        }
      }
    },
    {
      "Sid" : "AllowTaggingEC2ResourcesOnlyDuringInstanceCreation",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:*:ec2:*:*:instance/*",
        "arn:*:ec2:*:*:volume/*",
        "arn:*:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances"
          ]
        },
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "eks",
            "eks:cluster-name",
            "eks:nodegroup-name",
            "kubernetes.io/cluster/*"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSServiceRoleForAmazonQDeveloper

説明: このサービスリンクロールは、Amazon Q Developer の使用状況を提供する機能を提供します。

`AWSServiceRoleForAmazonQDeveloper` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2024 年 4 月 25 日 07:40 UTC
- 編集日時: 2024 年 4 月 25 日 07:40 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForAmazonQDeveloper`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "sid1",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/Q"
```

```
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSServiceRoleForAWSTransform

説明: このサービスにリンクされたロールは、 AWS Transform に使用状況情報を提供する機能を提供します。

AWSServiceRoleForAWSTransform は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2025 年 5 月 15 日 13:37 UTC
- 編集日時: 2025 年 12 月 1 日 13:19 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForAWSTransform

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PublishCloudWatchMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/Transform"
          ]
        }
      }
    },
    {
      "Sid" : "UserManagementPolicy",
      "Effect" : "Allow",
      "Action" : [
        "sso:DescribeApplication",
        "sso:GetApplicationAssignmentConfiguration",
        "sso:ListApplicationAssignmentsForPrincipal"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:*:sso:::instance/*"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityStore",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
"arn:*:identitystore::*:identitystore/*"
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SupportCaseManagement",
      "Effect" : "Allow",
      "Action" : [
        "support:CreateCase",
        "support:DescribeCases",
        "support:DescribeCommunications",
        "support:AddCommunicationToCase",
        "support:ResolveCase"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ExternalIdpSecretsAccess",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
```

```
      "Resource" : "arn:aws:secretsmanager:*:*:secret:transform!*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "transform",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy

説明: CloudWatch Alarms が使用する Systems Manager リソースへのアクセスを提供します

AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 10 月 1 日 09:49 UTC
- 編集日時: 2020 年 10 月 1 日 09:49 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ssm:CreateOpsItem"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePoli

説明: CloudWatch がユーザーに代わって RDS Performance Insights メトリクスにアクセスできるようにします。

`AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 9 月 7 日 09:32 UTC
- 編集日時: 2023 年 9 月 7 日 09:32 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "pi:GetResourceMetrics"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
```

```
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSServiceRoleForCodeGuru-Profiler

説明: Amazon CodeGuru Profiler がユーザーに代わって通知を送信するために必要となるサービスリンクロール。

`AWSServiceRoleForCodeGuru-Profiler` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 6 月 26 日 22:04 UTC
- 編集日時: 2020 年 6 月 26 日 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCodeGuru-Profiler`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSNSPublishToSendNotifications",
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSServiceRoleForCodeWhispererPolicy

説明: CodeWhisperer がアカウント内のデータにアクセスして請求額を計算する許可を付与し、Amazon CodeGuru でセキュリティレポートを作成およびアクセスするためのアクセスを提供して、CloudWatch にデータを送信します。

`AWSServiceRoleForCodeWhispererPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 3 月 24 日 19:39 UTC

- 編集日時: 2024 年 3 月 29 日 22:13 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCodeWhispererPolicy`

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
```

```
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSServiceRoleForEC2ScheduledInstances

説明: EC2 スケジュールインスタンスがスポットインスタンスを起動および管理できるようにします。

`AWSServiceRoleForEC2ScheduledInstances` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 10 月 12 日 18:31 UTC
- 編集日時: 2017 年 10 月 12 日 18:31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForEC2ScheduledInstances`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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" : "*"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy

説明: AWS GroundStation はこのサービスにリンクされたロールを使用して EC2 を呼び出し、パブリック IPv4 アドレスを検索します

AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 12 月 13 日 23:52 UTC
- 編集日時: 2022 年 12 月 13 日 23:52 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:DescribeAddresses",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSServiceRoleForImageBuilder

説明: EC2ImageBuilder がユーザーに代わって AWS サービスを呼び出すことを許可します。

AWSServiceRoleForImageBuilder は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 11 月 29 日 22:02 UTC
- 編集日時: 2025 年 7 月 23 日 16:52 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForImageBuilder

ポリシーのバージョン

ポリシーのバージョン: v21 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "ec2:RegisterImage",
      "Resource" : [
        "arn:aws:ec2:*::image/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:RegisterImage",
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-interface/*",
```

```
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:license-manager:*:*:license-configuration:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : [
            "EC2 Image Builder",
            "EC2 Fast Launch"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn",
            "vmie.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:StopInstances",
        "ec2:StartInstances",
        "ec2:TerminateInstances"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopyImage",
        "ec2:CreateImage",
        "ec2:CreateLaunchTemplate",
        "ec2:DeregisterImage",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:ModifyImageAttribute",
        "ec2:DescribeImportImageTasks",
        "ec2:DescribeExportImageTasks",
        "ec2:DescribeSnapshots",
        "ec2:DescribeHosts"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotAttribute"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances",
            "CreateImage"
          ],
          "aws:RequestTag/CreatedBy" : [
            "EC2 Image Builder",
            "EC2 Fast Launch"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:export-image-task/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : [
            "EC2 Image Builder",
            "EC2 Fast Launch"
          ]
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "license-manager:UpdateLicenseSpecificationsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListCommands",
        "ssm:ListCommandInvocations",
        "ssm:AddTagsToResource",
        "ssm:DescribeInstanceInformation",
        "ssm:GetAutomationExecution",
        "ssm:StopAutomationExecution",
        "ssm:ListInventoryEntries",
        "ssm:SendAutomationSignal",
        "ssm:DescribeInstanceAssociationsStatus",
        "ssm:DescribeAssociationExecutions",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-RunPowerShellScript",
        "arn:aws:ssm:*:*:document/AWS-RunShellScript",
        "arn:aws:ssm:*:*:document/AWSEC2-RunSysprep",
        "arn:aws:s3:::*"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ssm:resourceTag/CreatedBy" : [
            "EC2 Image Builder"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm: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-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:PutParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/imagebuilder/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter"
      ],
      "Resource" : "arn:aws:ssm:*::parameter/aws/service/*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSServiceRoleForIoTSiteWise

説明: AWS IoT SiteWise がゲートウェイをプロビジョニングおよび管理し、データをクエリできるようにします。このポリシーには、 グループにデプロイするために必要な AWS Greengrass アクセス許可、サービスプレフィックス付き関数を作成および更新するための AWS Lambda アクセス許可、およびデータストアからデータをクエリするための AWS IoT Analytics アクセス許可が含まれます。

`AWSServiceRoleForIoTSiteWise` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 11 月 14 日 19:19 UTC
- 編集日時: 2023 年 11 月 13 日 18:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForIoTSiteWise`

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSServiceRoleForLogDeliveryPolicy

説明: ログ配信サービスがユーザーに代わってログ配信先を呼び出してログを配信できるようにします。

AWSServiceRoleForLogDeliveryPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 10 月 4 日 17:31 UTC
- 編集日時: 2025 年 1 月 16 日 21:37 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForLogDeliveryPolicy

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LogDeliveryToFirehose",
      "Effect" : "Allow",
```

```
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch",
        "firehose:ListTagsForDeliveryStream"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/LogDeliveryEnabled" : "true"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSServiceRoleForMonitronPolicy

説明: ユーザーに代わって AWS SSO ユーザーの割り当てなど、 AWS リソースを管理するための Amazon Monitron アクセス許可を付与します。

AWSServiceRoleForMonitronPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 12 月 2 日 19:06 UTC
- 編集日時: 2024 年 10 月 2 日 10:06 UTC

- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForMonitronPolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sso:GetManagedApplicationInstance",
        "sso:GetProfile",
        "sso:ListProfiles",
        "sso:ListProfileAssociations",
        "sso:AssociateProfile",
        "sso:ListDirectoryAssociations",
        "sso-directory:DescribeUsers",
        "sso-directory:SearchUsers",
        "sso:CreateApplicationAssignment",
        "sso:ListApplicationAssignments"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSServiceRoleForNeptuneGraphPolicy

説明: Amazon Neptune の運用および使用状況に関するメトリクスとログを発行するための Cloudwatch アクセスを提供します

AWSServiceRoleForNeptuneGraphPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 11 月 29 日 14:03 UTC
- 編集日時: 2023 年 11 月 29 日 14:03 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForNeptuneGraphPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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}"
        }
      }
    }
  ]
```

```
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSServiceRoleForPrivateMarketplaceAdminPolicy

説明: Private Marketplace リソースを記述および更新し、 AWS Organizations を記述するアクセス許可を提供します

`AWSServiceRoleForPrivateMarketplaceAdminPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2024 年 2 月 14 日 22:28 UTC
- 編集日時: 2024 年 2 月 14 日 22:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForPrivateMarketplaceAdminPolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSServiceRoleForProcurementInsightsPolicy

説明: 調達インサイトが組織アカウントの詳細を取得するためのポリシー

AWSServiceRoleForProcurementInsightsPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2024 年 10 月 3 日 14:26 UTC
- 編集日時: 2024 年 10 月 3 日 14:26 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForProcurementInsightsPolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ProcurementInsightsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource" : [
        "*"
      ]
```

```
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSServiceRoleForSMS

説明: ECEC2, S3Cloudformation AWS を含む への AWS サービスインスタンスの移行に必要なサービスとリソースへのアクセスを提供します。

AWSServiceRoleForSMS は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 8 月 6 日 18:39 UTC
- 編集日時: 2020 年 10 月 15 日 17:28 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForSMS

ポリシーのバージョン

ポリシーのバージョン: v10 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSServiceRoleForUserSubscriptions

説明: お使いのアイデンティティセンターのリソースにユーザーサブスクリプションサービスへのアクセスを提供し、サブスクリプションを自動的に更新します。

AWSServiceRoleForUserSubscriptions は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2024 年 4 月 25 日 16:14 UTC
- 編集日時: 2025 年 10 月 29 日 14:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForUserSubscriptions`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SubscriptionManagementPolicy",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeGroup",
        "identitystore:DescribeUser",
        "identitystore:IsMemberInGroups",
        "identitystore:ListGroupMemberships",
        "organizations:DescribeOrganization",
        "sso:DescribeApplication",
        "sso:DescribeInstance",
        "sso:ListInstances",
        "sso-directory:DescribeUser"
```

```
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:*:sso:::instance/*"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityStore",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
 "arn:*:identitystore::*:identitystore/*"
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSServiceRolePolicyForBackupReports

説明: ユーザーに代わってコンプライアンスレポートを作成するための AWS Backup アクセス許可を提供します

AWSServiceRolePolicyForBackupReports は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 8 月 19 日 21:16 UTC
- 編集日時: 2023 年 3 月 10 日 00:51 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRolePolicyForBackupReports

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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*"
```

```
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSServiceRolePolicyForBackupRestoreTesting

説明: このポリシーには、リストアをテストしたり、テスト中に作成されたリソースをクリーンアップする許可が含まれています。

AWSServiceRolePolicyForBackupRestoreTesting は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 11 月 10 日 23:37 UTC
- 編集日時: 2024 年 2 月 14 日 22:42 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRolePolicyForBackupRestoreTesting

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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-*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSServiceRolePolicyForWorkspacesInstances

説明: この管理ポリシーは、Amazon WorkSpaces への管理アクセスを提供し、 の EC2 インスタンスを管理します。 AWS アカウント

AWSServiceRolePolicyForWorkspacesInstances は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2025 年 6 月 11 日 20:37 UTC
- 編集日時: 2025 年 6 月 11 日 20:37 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRolePolicyForWorkspacesInstances

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
```

```
        "ec2:DescribeVolumes"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances",
        "ec2:DeleteVolume",
        "ec2:StopInstances",
        "ec2:StartInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ManagedResourceOperator" : "workspaces-instances.amazonaws.com"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSShieldDRTAccessPolicy

説明: AWS DDoS レスポンスチームに への制限付きアクセスを提供し AWS アカウント 、重大度の高いイベント中の DDoS 攻撃の軽減を支援します。

AWSShieldDRTAccessPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSShieldDRTAccessPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー

- 作成日時: 2018 年 6 月 5 日 22:29 UTC
- 編集日時: 2020 年 12 月 15 日 17:28 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSShieldDRTAccessPolicy

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSShieldServiceRolePolicy

説明: Shield AWS がユーザーに代わって AWS リソースにアクセスして DDoS 保護を提供できるようにします。

AWSShieldServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 11 月 17 日 19:17 UTC
- 編集日時: 2021 年 11 月 17 日 19:17 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSShieldServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSShield",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:GetWebACL",
        "wafv2:UpdateWebACL",
        "wafv2:GetWebACLForResource",
        "wafv2:ListResourcesForWebACL",
        "cloudfront:ListDistributions",
        "cloudfront:GetDistribution"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSSocialMessagingServiceRolePolicy

説明: メトリクスを公開し、ソーシャルメッセージ送信に関するインサイトを提供するためのアクセス許可を提供します。

AWSSocialMessagingServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2024 年 10 月 10 日 19:28 UTC
- 編集日時: 2024 年 10 月 10 日 19:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSocialMessagingServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudwatchMetricPublishing",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/SocialMessaging"
        }
      }
    }
```

```
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSSSMForSAPServiceLinkedRolePolicy

説明: AWS Systems Manager for SAP に、SAP ソフトウェアを管理および統合するために必要なアクセス許可を提供します AWS。

`AWSSSMForSAPServiceLinkedRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 11 月 16 日 01:18 UTC
- 編集日時: 2025 年 8 月 12 日 23:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSSMForSAPServiceLinkedRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v13 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeInstanceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeRouteTables",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeVolumes",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVpcs",
        "ssm:GetCommandInvocation",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeInstanceStatus",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeInstanceStatus",
      "Resource" : "*"
    },
    {
      "Sid" : "TargetRuleActions",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:PutTargets",
        "events:DescribeRule",
        "events:PutRule",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:*:events:*:*:rule/SSMSAPManagedRule*",
        "arn:*:events:*:*:event-bus/default"
      ]
    },
    {
```

```
      "Sid" : "DocumentActions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument",
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:*:ssm:*:*:document/AWSSystemsManagerSAP-*",
        "arn:*:ssm:*:*:document/AWSSSMSAP*",
        "arn:*:ssm:*:*:document/AWSSAP*"
      ]
    },
    {
      "Sid" : "CustomerSendCommand",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:*:ec2:*:*:instance/*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "ssm:resourceTag/SSMForSAPManaged" : "True"
        }
      }
    },
    {
      "Sid" : "InstanceTagActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:*:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/awsApplication" : "false"
        },
        "StringEqualsIgnoreCase" : {
          "ec2:ResourceTag/SSMForSAPManaged" : "True"
        }
      }
    },
    {
      "Sid" : "DescribeTag",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeTags",
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "GetApplication",
      "Effect" : "Allow",
      "Action" : "servicecatalog:GetApplication",
      "Resource" : "arn:*:servicecatalog:*:*:*"
    },
    {
      "Sid" : "UpdateOrDeleteApplication",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:DeleteApplication",
        "servicecatalog:UpdateApplication"
      ],
      "Resource" : "arn:*:servicecatalog:*:*:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SSMForSAPCreated" : "True"
        }
      }
    },
    {
      "Sid" : "CreateApplication",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:TagResource",
        "servicecatalog:CreateApplication"
      ],
      "Resource" : "arn:*:servicecatalog:*:*:*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SSMForSAPCreated" : "True"
        }
      }
    },
    {
      "Sid" : "CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/servicecatalog-
appregistry.amazonaws.com/AWSServiceRoleForAWSServiceCatalogAppRegistry",
      "Condition" : {
        "StringEquals" : {
```

```
          "iam:AWSServiceName" : "servicecatalog-appregistry.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PutMetricData",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/Usage",
            "AWS/SSMForSAP"
          ]
        }
      }
    },
    {
      "Sid" : "CreateAttributeGroup",
      "Effect" : "Allow",
      "Action" : "servicecatalog:CreateAttributeGroup",
      "Resource" : "arn:*:servicecatalog:*:*:/attribute-groups/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SSMForSAPCreated" : "True"
        }
      }
    },
    {
      "Sid" : "GetAttributeGroup",
      "Effect" : "Allow",
      "Action" : "servicecatalog:GetAttributeGroup",
      "Resource" : "arn:*:servicecatalog:*:*:/attribute-groups/*"
    },
    {
      "Sid" : "DeleteAttributeGroup",
      "Effect" : "Allow",
      "Action" : "servicecatalog:DeleteAttributeGroup",
      "Resource" : "arn:*:servicecatalog:*:*:/attribute-groups/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SSMForSAPCreated" : "True"
        }
```

```
      }
    },
    {
      "Sid" : "AttributeGroupActions",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:AssociateAttributeGroup",
        "servicecatalog:DisassociateAttributeGroup"
      ],
      "Resource" : "arn:*:servicecatalog:*:*:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SSMForSAPCreated" : "True"
        }
      }
    },
    {
      "Sid" : "ListAssociatedAttributeGroups",
      "Effect" : "Allow",
      "Action" : "servicecatalog:ListAssociatedAttributeGroups",
      "Resource" : "arn:*:servicecatalog:*:*:*"
    },
    {
      "Sid" : "CreateGroup",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:Tag"
      ],
      "Resource" : "arn:*:resource-groups:*:*:group/SystemsManagerForSAP-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SSMForSAPCreated" : "True"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SSMForSAPCreated"
          ]
        }
      }
    },
    {
      "Sid" : "GetGroup",
      "Effect" : "Allow",
```

```
      "Action" : "resource-groups:GetGroup",
      "Resource" : "arn:*:resource-groups:*:*:group/SystemsManagerForSAP-*"
    },
    {
      "Sid" : "DeleteGroup",
      "Effect" : "Allow",
      "Action" : "resource-groups:DeleteGroup",
      "Resource" : "arn:*:resource-groups:*:*:group/SystemsManagerForSAP-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SSMForSAPCreated" : "True"
        }
      }
    },
    {
      "Sid" : "CreateAppTagResourceGroup",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup"
      ],
      "Resource" : "arn:*:resource-groups:*:*:group/AWS_AppRegistry_AppTag_*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/EnableAWSServiceCatalogAppRegistry" : "true"
        }
      }
    },
    {
      "Sid" : "TagAppTagResourceGroup",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:Tag"
      ],
      "Resource" : "arn:*:resource-groups:*:*:group/AWS_AppRegistry_AppTag_*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/EnableAWSServiceCatalogAppRegistry" : "true"
        }
      }
    },
    {
      "Sid" : "GetAppTagResourceGroupConfig",
      "Effect" : "Allow",
      "Action" : [
```

```
        "resource-groups:GetGroupConfiguration"
      ],
      "Resource" : [
        "arn:*:resource-groups:*:*:group/AWS_AppRegistry_AppTag_*"
      ]
    },
    {
      "Sid" : "StartStopInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "Resource" : "arn:*:ec2:*:*:instance/*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "ec2:resourceTag/SSMForSAPManaged" : "True"
        }
      }
    },
    {
      "Sid" : "SsmSapResourceGroup",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:Tag",
        "resource-groups:CreateGroup"
      ],
      "Resource" : "arn:aws:resource-groups:*:*:group/SystemsManagerForSAP-*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SSMForSAPCreated" : "True"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SSMForSAPCreated"
          ]
        }
      }
    },
    {
      "Sid" : "ManageSsmSapTagsOnEc2Instances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
```

```
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SSMForSAPManaged" : "True"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "SystemsManagerForSAP-*"
          ]
        }
      }
    },
    {
      "Sid" : "ManageSsmSapTagsOnEbsVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "SystemsManagerForSAP-*"
          ]
        }
      }
    },
    {
      "Sid" : "ManageAppTagsOnEbsVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "ArnLike" : {
          "aws:RequestTag/awsApplication" : "arn:aws:resource-groups:*:*:group/*/*"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
```

```
            "awsApplication"
          ]
        }
      }
    },
    {
      "Sid" : "ManageCostAllocationTags",
      "Effect" : "Allow",
      "Action" : [
        "ce:ListCostAllocationTags",
        "ce:UpdateCostAllocationTagsStatus",
        "ce:ListCostAllocationTagBackfillHistory",
        "ce:StartCostAllocationTagBackfill"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSSSMOpsInsightsServiceRolePolicy

説明: サービスリンクロール「AWSServiceRoleForAmazonSSM_OpsInsights」に関するポリシー

AWSSSMOpsInsightsServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 6 月 16 日 20:12 UTC

- 編集日時: 2021 年 6 月 16 日 20:12 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSSSMOpsInsightsServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
```

```
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSSSODirectoryAdministrator

説明: SSO ディレクトリへの管理者アクセス

AWSSSODirectoryAdministrator は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSSSODirectoryAdministrator をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 10 月 31 日 23:54 UTC
- 編集日時: 2025 年 9 月 16 日 19:49 UTC
- ARN: arn:aws:iam::aws:policy/AWSSSODirectoryAdministrator

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Sid" : "AWSSSODirectoryAdministrator",
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:*",
        "identitystore:*",
        "identitystore-auth:*",
        "sso:ListDirectoryAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowKMSKeyUseViaAWSIdentityStoreService",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com",
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" : "*"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSSSODirectoryReadOnly

説明: SSO ディレクトリへの読み取り専用アクセス

AWSSSODirectoryReadOnly は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSSSODirectoryReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 10 月 31 日 23:49 UTC
- 編集日時: 2025 年 9 月 16 日 19:49 UTC
- ARN: arn:aws:iam::aws:policy/AWSSSODirectoryReadOnly

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSSODirectoryReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:Search*",
        "sso-directory:Describe*",
        "sso-directory:List*",
        "sso-directory:Get*",
        "identitystore:Describe*",
        "identitystore:List*",
        "identitystore-auth:ListSessions",
        "identitystore-auth:BatchGetSession"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "AllowKMSKeyUseViaAWSIdentityStoreService",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com",
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" : "*"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSSSOMasterAccountAdministrator

説明: AWS Organizations のマスターアカウントとメンバーアカウント、およびクラウドアプリケーションを管理するための SSO AWS 内のアクセスを提供します

`AWSSSOMasterAccountAdministrator` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSSSOMasterAccountAdministrator` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 6 月 27 日 20:36 UTC

- 編集日時: 2025 年 9 月 16 日 19:49 UTC
- ARN: arn:aws:iam::aws:policy/AWSSSOMasterAccountAdministrator

ポリシーのバージョン

ポリシーのバージョン: v11 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSSOCreateSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/
AWSServiceRoleForSSO",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "sso.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AWSSSOMasterAccountAdministrator",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/
AWSServiceRoleForSSO",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "sso.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AWSSSOMemberAccountAdministrator",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ds:DescribeTrusts",
        "ds:UnauthorizeApplication",
        "ds:DescribeDirectories",
        "ds:AuthorizeApplication",
        "iam:ListPolicies",
        "organizations:EnableAWSServiceAccess",
        "organizations:ListRoots",
        "organizations:ListAccounts",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAccountsForParent",
        "organizations:DescribeOrganization",
        "organizations:ListChildren",
        "organizations:DescribeAccount",
        "organizations:ListParents",
        "organizations:ListDelegatedAdministrators",
        "sso:*",
        "sso-directory:*",
        "identitystore:*",
        "identitystore-auth:*",
        "ds:CreateAlias",
        "access-analyzer:ValidatePolicy",
        "signin:CreateTrustedIdentityPropagationApplicationForConsole",
        "signin:ListTrustedIdentityPropagationApplicationsForConsole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSSSOManageDelegatedAdministrator",
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "sso.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowDeleteSyncProfile",
```

```
      "Effect" : "Allow",
      "Action" : [
        "identity-sync:DeleteSyncProfile"
      ],
      "Resource" : [
        "arn:aws:identity-sync:*:*:profile/*"
      ]
    },
    {
      "Sid" : "AllowKMSKeyUseViaAWSIAMIdentityCenterService",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Encrypt",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com",
          "kms:EncryptionContext:aws:sso:instance-arn" : "*"
        }
      }
    },
    {
      "Sid" : "AllowKMSKeyUseViaAWSIdentityStoreService",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Encrypt",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com",
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" : "*"
        }
      }
    },
    {
      "Sid" : "AllowKMSKeyDiscovery",
      "Effect" : "Allow",
      "Action" : [
```

```
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSSSOMemberAccountAdministrator

説明: AWS Organizations メンバーアカウントとクラウドアプリケーションを管理するための SSO AWS 内のアクセスを提供します

`AWSSSOMemberAccountAdministrator` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSSSOMemberAccountAdministrator` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 6 月 27 日 20:45 UTC
- 編集日時: 2025 年 9 月 16 日 19:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSSOMemberAccountAdministrator`

ポリシーのバージョン

ポリシーのバージョン: v9 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSSOMemberAccountAdministrator",
      "Effect" : "Allow",
      "Action" : [
        "ds:DescribeDirectories",
        "ds:AuthorizeApplication",
        "ds:UnauthorizeApplication",
        "ds:DescribeTrusts",
        "iam:ListPolicies",
        "organizations:EnableAWSServiceAccess",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "organizations:ListRoots",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListParents",
        "organizations:ListChildren",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListDelegatedAdministrators",
        "sso:*",
        "sso-directory:*",
        "identitystore:*",
        "identitystore-auth:*",
        "ds:CreateAlias",
        "access-analyzer:ValidatePolicy",
        "signin:CreateTrustedIdentityPropagationApplicationForConsole",
        "signin:ListTrustedIdentityPropagationApplicationsForConsole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSSSOManageDelegatedAdministrator",
      "Effect" : "Allow",
      "Action" : [
```

```
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "sso.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowKMSKeyUseViaAWSIAMIdentityCenterService",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Encrypt",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com",
          "kms:EncryptionContext:aws:sso:instance-arn" : "*"
        }
      }
    },
    {
      "Sid" : "AllowKMSKeyUseViaAWSIdentityStoreService",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Encrypt",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com",
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" : "*"
        }
      }
    },
    {
      "Sid" : "AllowKMSKeyDiscovery",
```

```
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSSSOReadOnly

説明: SSO AWS 設定への読み取り専用アクセスを提供します。

`AWSSSOReadOnly` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSSSOReadOnly` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 6 月 27 日 20:24 UTC
- 編集日時: 2025 年 9 月 16 日 19:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSSOReadOnly`

ポリシーのバージョン

ポリシーのバージョン: v10 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSSOReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "ds:DescribeDirectories",
        "ds:DescribeTrusts",
        "iam:ListPolicies",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "organizations:ListParents",
        "organizations:ListChildren",
        "organizations:ListAccounts",
        "organizations:ListRoots",
        "organizations:ListAccountsForParent",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListDelegatedAdministrators",
        "sso:Describe*",
        "sso:Get*",
        "sso:List*",
        "sso:Search*",
        "sso-directory:DescribeDirectory",
        "access-analyzer:ValidatePolicy",
        "signin:ListTrustedIdentityPropagationApplicationsForConsole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowKMSKeyUseViaAWSIAMIdentityCenterService",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com",
          "kms:EncryptionContext:aws:sso:instance-arn" : "*"
        }
      }
    },
    {
      "Sid" : "AllowKMSKeyDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSSSOServiceRolePolicy

説明: ユーザーに代わって AWS IAM ロール、ポリシー、SAML IdP などの AWS リソースを管理する SSO アクセス許可を付与します。

AWSSSOServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 12 月 5 日 18:36 UTC
- 編集日時: 2025 年 2 月 11 日 18:37 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSSSOServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v18 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IAMRoleProvisioningActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:CreateRole",
        "iam:PutRolePolicy",
        "iam:UpdateRole",
        "iam:UpdateRoleDescription",
        "iam:UpdateAssumeRolePolicy",
        "iam:PutRolePermissionsBoundary",
        "iam:DeleteRolePermissionsBoundary"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-reserved/sso.amazonaws.com/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalOrgMasterAccountId" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "IAMRoleReadActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRoles"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "IAMRoleCleanupActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-reserved/sso.amazonaws.com/*"
      ]
    },
    {
      "Sid" : "IAMSLRCleanupActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus",
        "iam:DeleteRole",
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/AWSServiceRoleForSSO"
      ]
    },
    {
      "Sid" : "IAMSAMLProviderCreationAction",
      "Effect" : "Allow",
      "Action" : [
```

```
        "iam:CreateSAMLProvider"
      ],
      "Resource" : [
        "arn:aws:iam::*:saml-provider/AWSSSO_*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalOrgMasterAccountId" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "IAMSAMLProviderUpdateAction",
      "Effect" : "Allow",
      "Action" : [
        "iam:UpdateSAMLProvider"
      ],
      "Resource" : [
        "arn:aws:iam::*:saml-provider/AWSSSO_*"
      ]
    },
    {
      "Sid" : "IAMSAMLProviderCleanupActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteSAMLProvider",
        "iam:GetSAMLProvider"
      ],
      "Resource" : [
        "arn:aws:iam::*:saml-provider/AWSSSO_*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : [
        "*"
      ]
```

```
    },
    {
      "Sid" : "AllowUnauthAppForDirectory",
      "Effect" : "Allow",
      "Action" : [
        "ds:UnauthorizeApplication"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowDescribeForDirectory",
      "Effect" : "Allow",
      "Action" : [
        "ds:DescribeDirectories",
        "ds:DescribeTrusts"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowDescribeAndListOperationsOnIdentitySource",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeUser",
        "identitystore:DescribeGroup",
        "identitystore:ListGroups",
        "identitystore:ListUsers"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowDeleteSyncProfile",
      "Effect" : "Allow",
      "Action" : [
        "identity-sync:DeleteSyncProfile"
      ],
      "Resource" : [
        "arn:aws:identity-sync:*:*:profile/*"
      ]
```

```
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSStepFunctionsConsoleFullAccess

説明: user/role/etcに AWS StepFunctions コンソールへのアクセスを提供するアクセスポリシー。コンソールをフルに活用するには、このポリシーに加えて、ユーザーはサービスが引き受けることが可能な他の IAM ロールに iam:PassRole 許可が必要な場合があります。

`AWSStepFunctionsConsoleFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSStepFunctionsConsoleFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 1 月 11 日 21:54 UTC
- 編集日時: 2017 年 1 月 12 日 00:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStepFunctionsConsoleFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSStepFunctionsFullAccess

説明: AWS StepFunctions API へのアクセスをuser/role/etcに提供するためのアクセスポリシー。フルアクセスを得るには、このポリシーに加えて、ユーザーはサービスが引き受けることが可能な IAM ロールを最低 1 つでも iam:PassRole 許可が付与される必要があります。

AWSStepFunctionsFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSStepFunctionsFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 1 月 11 日 21:51 UTC
- 編集日時: 2017 年 1 月 11 日 21:51 UTC
- ARN: arn:aws:iam::aws:policy/AWSStepFunctionsFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "states:*",
      "Resource" : "*"
    }
```

```
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSStepFunctionsReadOnlyAccess

説明: user/role/etcに AWS StepFunctions サービスへの読み取り専用アクセスを提供するアクセスポリシー。

`AWSStepFunctionsReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSStepFunctionsReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 1 月 11 日 21:46 UTC
- 編集日時: 2024 年 4 月 26 日 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStepFunctionsReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSStorageGatewayFullAccess

説明: 経由で AWS Storage Gatewayへのフルアクセスを提供します AWS マネジメントコンソール。

AWSStorageGatewayFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSStorageGatewayFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2022 年 9 月 6 日 20:26 UTC
- ARN: arn:aws:iam::aws:policy/AWSStorageGatewayFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSStorageGatewayReadOnlyAccess

説明: 経由で AWS Storage Gatewayへのアクセスを提供します AWS マネジメントコンソール。

`AWSStorageGatewayReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSStorageGatewayReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2022 年 9 月 6 日 20:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStorageGatewayReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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/*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSStorageGatewayServiceRolePolicy

説明: 他の サービスと Storage AWS Gateway の統合を可能にするために、Storage Storage Gateway で使用される AWS サービスにリンクされたロール。

`AWSStorageGatewayServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 2 月 17 日 19:03 UTC
- 編集日時: 2021 年 2 月 17 日 19:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSStorageGatewayServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "fsx:ListTagsForResource"
      ],
```

```
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSSupplyChainFederationAdminAccess

説明: AWSSupplyChainFederationAdminAccess は AWS 、 Supply Chain AWS アプリケーション内でアクションを実行するために必要なアクセス許可など、 Supply Chain フェデレーティッドユーザーに AWS Supply Chain アプリケーションへのアクセスを提供します。このポリシーは、IAM Identity Center のユーザーとグループに対する管理アクセス許可を提供し、ユーザーに代わって AWS Supply Chain によって作成されたロールにアタッチされます。その他の IAM エンティティに AWSSupplyChainFederationAdminAccess ポリシーをアタッチしないでください。

`AWSSupplyChainFederationAdminAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSSupplyChainFederationAdminAccess` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 3 月 1 日 18:54 UTC
- 編集日時: 2025 年 10 月 30 日 21:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSSupplyChainFederationAdminAccess`

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSupplyChain",
      "Effect" : "Allow",
      "Action" : [
        "scn:*"
      ],
      "Resource" : [
        "arn:aws:scn:*:*:instance/*"
      ]
    },
    {
      "Sid" : "ChimeAppInstance",
      "Effect" : "Allow",
      "Action" : [
        "chime:BatchCreateChannelMembership",
        "chime:CreateAppInstanceUser",
        "chime:CreateChannel",
        "chime:CreateChannelMembership",
        "chime:CreateChannelModerator",
        "chime:Connect",
        "chime:DeleteChannelMembership",
        "chime:DeleteChannelModerator",
        "chime:DescribeChannelMembershipForAppInstanceUser",
        "chime:GetChannelMembershipPreferences",
        "chime:ListChannelMemberships",
        "chime:ListChannelMembershipsForAppInstanceUser",
        "chime:ListChannelMessages",
        "chime:ListChannelModerators",
        "chime:TagResource",
        "chime:PutChannelMembershipPreferences",
        "chime:SendChannelMessage",
        "chime:UpdateChannelReadMarker",
        "chime:UpdateAppInstanceUser"
      ],
```

```
      "Resource" : [
        "arn:aws:chime:*:*:app-instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/SCNInstanceId" : "*"
        }
      }
    },
    {
      "Sid" : "ChimeChannel",
      "Effect" : "Allow",
      "Action" : [
        "chime:DescribeChannel"
      ],
      "Resource" : [
        "arn:aws:chime:*:*:app-instance/*"
      ]
    },
    {
      "Sid" : "ChimeMessaging",
      "Effect" : "Allow",
      "Action" : [
        "chime:GetMessagingSessionEndpoint"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
        "sso:GetManagedApplicationInstance",
        "sso:ListDirectoryAssociations",
        "sso:AssociateProfile",
        "sso:DisassociateProfile",
        "sso:ListProfiles",
        "sso:GetProfile",
        "sso:ListProfileAssociations",
        "sso:ListApplicationAssignments",
        "sso:DescribeApplication",
        "sso:DescribeInstance",
        "sso:GetApplicationAssignmentConfiguration"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "AppflowConnectorProfile",
      "Effect" : "Allow",
      "Action" : [
        "appflow:CreateConnectorProfile",
        "appflow:UseConnectorProfile",
        "appflow:DeleteConnectorProfile",
        "appflow:UpdateConnectorProfile"
      ],
      "Resource" : [
        "arn:aws:appflow:*:*:connectorprofile/scn-*"
      ]
    },
    {
      "Sid" : "AppflowFlow",
      "Effect" : "Allow",
      "Action" : [
        "appflow:CreateFlow",
        "appflow:DeleteFlow",
        "appflow:DescribeFlow",
        "appflow:DescribeFlowExecutionRecords",
        "appflow:ListFlows",
        "appflow:StartFlow",
        "appflow:StopFlow",
        "appflow:UpdateFlow",
        "appflow:TagResource",
        "appflow:UntagResource"
      ],
      "Resource" : [
        "arn:aws:appflow:*:*:flow/scn-*"
      ]
    },
    {
      "Sid" : "S3ListAllBuckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3ListSupplyChainBucket",
      "Effect" : "Allow",
```

```
      "Action" : [
        "s3:GetBucketLocation",
        "s3:GetBucketPolicy",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-supply-chain-data-*"
      ]
    },
    {
      "Sid" : "S3ReadWriteObject",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-supply-chain-data-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SecretsManagerCreateSecret",
      "Effect" : "Allow",
      "Action" : "secretsmanager:CreateSecret",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:Name" : "appflow!*"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "appflow.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "SecretsManagerPutResourcePolicy",
      "Effect" : "Allow",
```

```
      "Action" : [
        "secretsmanager:PutResourcePolicy"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "appflow.amazonaws.com"
          ]
        },
        "StringEqualsIgnoreCase" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "appflow"
        }
      }
    },
    {
      "Sid" : "KMSListKeys",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
        "kms:ListAliases"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
      "Sid" : "KMSListGrants",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListGrants"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "appflow.*.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceTag/aws-supply-chain-access" : "true"
        }
      }
    },
    {
      "Sid" : "KMSCreateGrant",
      "Effect" : "Allow",
```

```
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "appflow.*.amazonaws.com"
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        },
        "StringEquals" : {
          "aws:ResourceTag/aws-supply-chain-access" : "true"
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:*:sso:::instance/*"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityStore",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
"arn:*:identitystore::*:identitystore/*"
        },
```

```
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSSupportAccess

説明: ユーザーに AWS サポート センターへのアクセスを許可します。

AWSSupportAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSSupportAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2025 年 7 月 18 日 13:52 UTC
- ARN: arn:aws:iam::aws:policy/AWSSupportAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "support:*",
        "support-console:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSSupportAppFullAccess

説明: AWS サポート アプリと、 AWS サポート や Service Quotas などの他の必要なサービスへのフルアクセスを提供します。このポリシーには、ユーザーがサポートケース AWS サポート の問い合わせ、サービスクォータの変更、関連するサービスにリンクされたロールの作成を行えるように、サポートサービスを使用するアクセス許可が含まれています。

`AWSSupportAppFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSSupportAppFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 8 月 22 日 16:53 UTC
- 編集日時: 2022 年 8 月 22 日 16:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportAppFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSSupportAppReadOnlyAccess

説明: AWS サポート アプリへの読み取り専用アクセスを提供します。

`AWSSupportAppReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSSupportAppReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 8 月 22 日 17:01 UTC
- 編集日時: 2022 年 8 月 22 日 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportAppReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "support:DescribeCases",
        "support:DescribeCommunications"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSSupportPlansFullAccess

説明: サポートプランへのフルアクセスを提供します。

AWSSupportPlansFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSSupportPlansFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 9 月 27 日 18:19 UTC
- 編集日時: 2024 年 9 月 9 日 21:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportPlansFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "supportplans:GetSupportPlan",
        "supportplans:GetSupportPlanUpdateStatus",
        "supportplans:ListSupportPlanModifiers",
        "supportplans:StartSupportPlanUpdate",
        "supportplans:CreateSupportPlanSchedule"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSSupportPlansReadOnlyAccess

説明: サポートプランへの読み取り専用アクセスを提供します。

AWSSupportPlansReadOnlyAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSSupportPlansReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 9 月 27 日 18:08 UTC
- 編集日時: 2024 年 9 月 9 日 21:21 UTC
- ARN: arn:aws:iam::aws:policy/AWSSupportPlansReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "supportplans:GetSupportPlan",
        "supportplans:GetSupportPlanUpdateStatus",
```

```
        "supportplans:ListSupportPlanModifiers"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSSupportServiceRolePolicy

説明: AWS サポート が AWS リソースにアクセスして、請求、管理、サポートサービスを提供できるようにします。

AWSSupportServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 4 月 19 日 18:04 UTC
- 編集日時: 2025 年 12 月 8 日 23:04 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSSupportServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v43 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Statement" : [
    {
      "Sid" : "AWSSupportAPIGatewayAccess",
      "Action" : [
        "apigateway:GET"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:apigateway:*::/account",
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/apis/*/authorizers",
        "arn:aws:apigateway:*::/apis/*/authorizers/*",
        "arn:aws:apigateway:*::/apis/*/deployments",
        "arn:aws:apigateway:*::/apis/*/deployments/*",
        "arn:aws:apigateway:*::/apis/*/integrations",
        "arn:aws:apigateway:*::/apis/*/integrations/*",
        "arn:aws:apigateway:*::/apis/*/integrations/*/integrationresponses",
        "arn:aws:apigateway:*::/apis/*/integrations/*/integrationresponses/*",
        "arn:aws:apigateway:*::/apis/*/models",
        "arn:aws:apigateway:*::/apis/*/models/*",
        "arn:aws:apigateway:*::/apis/*/routes",
        "arn:aws:apigateway:*::/apis/*/routes/*",
        "arn:aws:apigateway:*::/apis/*/routes/*/routeresponses",
        "arn:aws:apigateway:*::/apis/*/routes/*/routeresponses/*",
        "arn:aws:apigateway:*::/apis/*/stages",
        "arn:aws:apigateway:*::/apis/*/stages/*",
        "arn:aws:apigateway:*::/clientcertificates",
        "arn:aws:apigateway:*::/clientcertificates/*",
        "arn:aws:apigateway:*::/domainnames",
        "arn:aws:apigateway:*::/domainnames/*",
        "arn:aws:apigateway:*::/domainnames/*/apimappings",
        "arn:aws:apigateway:*::/domainnames/*/apimappings/*",
        "arn:aws:apigateway:*::/domainnames/*/basepathmappings",
        "arn:aws:apigateway:*::/domainnames/*/basepathmappings/*",
        "arn:aws:apigateway:*::/restapis",
```

```
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/restapis/*/authorizers",
        "arn:aws:apigateway:*::/restapis/*/authorizers/*",
        "arn:aws:apigateway:*::/restapis/*/deployments",
        "arn:aws:apigateway:*::/restapis/*/deployments/*",
        "arn:aws:apigateway:*::/restapis/*/models",
        "arn:aws:apigateway:*::/restapis/*/models/*",
        "arn:aws:apigateway:*::/restapis/*/models/*/default_template",
        "arn:aws:apigateway:*::/restapis/*/resources",
        "arn:aws:apigateway:*::/restapis/*/resources/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integration/responses/
*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/responses/*",
        "arn:aws:apigateway:*::/restapis/*/stages/*/sdks/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integration",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/usageplans",
        "arn:aws:apigateway:*::/usageplans/*",
        "arn:aws:apigateway:*::/vpclinks",
        "arn:aws:apigateway:*::/vpclinks/*"
      ]
    },
    {
      "Sid" : "AWSSupportDeleteRoleAccess",
      "Action" : [
        "iam:DeleteRole"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/support.amazonaws.com/
AWSServiceRoleForSupport"
      ]
    },
    {
      "Sid" : "AWSSupportActionsGroup1",
      "Action" : [
        "access-analyzer:getAccessPreview",
        "access-analyzer:getAnalyzedResource",
        "access-analyzer:getAnalyzer",
        "access-analyzer:getArchiveRule",
        "access-analyzer:getFinding",
        "access-analyzer:getGeneratedPolicy",
```

```
        "access-analyzer:listAccessPreviewFindings",
        "access-analyzer:listAccessPreviews",
        "access-analyzer:listAnalyzedResources",
        "access-analyzer:listAnalyzers",
        "access-analyzer:listArchiveRules",
        "access-analyzer:listFindings",
        "access-analyzer:listPolicyGenerations",
        "account:getRegionOptStatus",
        "account:listRegions",
        "acm-pca:describeCertificateAuthority",
        "acm-pca:describeCertificateAuthorityAuditReport",
        "acm-pca:getCertificate",
        "acm-pca:getCertificateAuthorityCertificate",
        "acm-pca:getCertificateAuthorityCsr",
        "acm-pca:listCertificateAuthorities",
        "acm-pca:listTags",
        "acm:describeCertificate",
        "acm:getAccountConfiguration",
        "acm:getCertificate",
        "acm:listCertificates",
        "acm:listTagsForCertificate",
        "aiops:getInvestigationGroup",
        "aiops:getInvestigationGroupPolicy",
        "aiops:listInvestigationGroups",
        "airflow:getEnvironment",
        "airflow:listEnvironments",
        "airflow:listTagsForResource",
        "amplify:getApp",
        "amplify:getBackendEnvironment",
        "amplify:getBranch",
        "amplify:getDomainAssociation",
        "amplify:getJob",
        "amplify:getWebhook",
        "amplify:listApps",
        "amplify:listBackendEnvironments",
        "amplify:listBranches",
        "amplify:listDomainAssociations",
        "amplify:listJobs",
        "amplify:listWebhooks",
        "amplifyuibuilder:exportComponents",
        "amplifyuibuilder:exportThemes",
        "aoss:batchGetCollection",
        "aoss:batchGetEffectiveLifecyclePolicy",
        "aoss:batchGetLifecyclePolicy",
```

```
        "aoss:batchGetVpcEndpoint",
        "aoss:getAccessPolicy",
        "aoss:getAccountSettings",
        "aoss:getPoliciesStats",
        "aoss:getSecurityConfig",
        "aoss:getSecurityPolicy",
        "aoss:listAccessPolicies",
        "aoss:listCollections",
        "aoss:listLifecyclePolicies",
        "aoss:listSecurityConfigs",
        "aoss:listSecurityPolicies",
        "aoss:listTagsForResource",
        "aoss:listVpcEndpoints",
        "appconfig:getApplication",
        "appconfig:getConfigurationProfile",
        "appconfig:getDeployment",
        "appconfig:getDeploymentStrategy",
        "appconfig:getEnvironment",
        "appconfig:getExtension",
        "appconfig:getExtensionAssociation",
        "appconfig:listApplications",
        "appconfig:listConfigurationProfiles",
        "appconfig:listDeployments",
        "appconfig:listDeploymentStrategies",
        "appconfig:listEnvironments",
        "appconfig:listExtensionAssociations",
        "appconfig:listExtensions",
        "appconfig:listHostedConfigurationVersions",
        "appflow:describeConnectorEntity",
        "appflow:describeConnectorProfiles",
        "appflow:describeConnectors",
        "appflow:describeFlow",
        "appflow:describeFlowExecutionRecords",
        "appflow:listConnectorEntities",
        "appflow:listFlows",
        "application-autoscaling:describeScalableTargets",
        "application-autoscaling:describeScalingActivities",
        "application-autoscaling:describeScalingPolicies",
        "application-autoscaling:describeScheduledActions",
        "application-signals:getService",
        "application-signals:getServiceLevelObjective",
        "application-signals:listServiceDependencies",
        "application-signals:listServiceDependents",
        "application-signals:listServiceLevelObjectives",
```

```
        "application-signals:listServiceOperations",
        "application-signals:listServices",
        "applicationinsights:describeApplication",
        "applicationinsights:describeComponent",
        "applicationinsights:describeComponentConfiguration",
        "applicationinsights:describeComponentConfigurationRecommendation",
        "applicationinsights:describeLogPattern",
        "applicationinsights:describeObservation",
        "applicationinsights:describeProblem",
        "applicationinsights:describeProblemObservations",
        "applicationinsights:listApplications",
        "applicationinsights:listComponents",
        "applicationinsights:listConfigurationHistory",
        "applicationinsights:listLogPatterns",
        "applicationinsights:listLogPatternSets",
        "applicationinsights:listProblems",
        "appmesh:describeGatewayRoute",
        "appmesh:describeMesh",
        "appmesh:describeRoute",
        "appmesh:describeVirtualGateway",
        "appmesh:describeVirtualNode",
        "appmesh:describeVirtualRouter",
        "appmesh:describeVirtualService",
        "appmesh:listGatewayRoutes",
        "appmesh:listMeshes",
        "appmesh:listRoutes",
        "appmesh:listTagsForResource",
        "appmesh:listVirtualGateways",
        "appmesh:listVirtualNodes",
        "appmesh:listVirtualRouters",
        "appmesh:listVirtualServices",
        "apprunner:describeAutoScalingConfiguration",
        "apprunner:describeCustomDomains",
        "apprunner:describeObservabilityConfiguration",
        "apprunner:describeOperation",
        "apprunner:describeService",
        "apprunner:describeVpcConnector",
        "apprunner:describeVpcIngressConnection",
        "apprunner:listAutoScalingConfigurations",
        "apprunner:listConnections",
        "apprunner:listObservabilityConfigurations",
        "apprunner:listOperations",
        "apprunner:listServices",
        "apprunner:listTagsForResource",
```

```
        "apprunner:listVpcConnectors",
        "apprunner:listVpcIngressConnections",
        "appstream:describeAppBlockBuilderAppBlockAssociations",
        "appstream:describeAppBlockBuilders",
        "appstream:describeAppBlocks",
        "appstream:describeApplicationFleetAssociations",
        "appstream:describeApplications",
        "appstream:describeDirectoryConfigs",
        "appstream:describeEntitlements",
        "appstream:describeFleets",
        "appstream:describeImageBuilders",
        "appstream:describeImagePermissions",
        "appstream:describeImages",
        "appstream:describeSessions",
        "appstream:describeStacks",
        "appstream:describeUsageReportSubscriptions",
        "appstream:describeUsers",
        "appstream:describeUserStackAssociations",
        "appstream:listAssociatedFleets",
        "appstream:listAssociatedStacks",
        "appstream:listEntitledApplications",
        "appstream:listTagsForResource",
        "appsync:evaluateCode",
        "appsync:evaluateMappingTemplate",
        "appsync:getApi",
        "appsync:getApiAssociation",
        "appsync:getApiCache",
        "appsync:getChannelNamespace",
        "appsync:getDataSource",
        "appsync:getDataSourceIntrospection",
        "appsync:getDomainName",
        "appsync:getFunction",
        "appsync:getGraphqlApi",
        "appsync:getGraphqlApiEnvironmentVariables",
        "appsync:getIntrospectionSchema",
        "appsync:getResolver",
        "appsync:getSchemaCreationStatus",
        "appsync:getSourceApiAssociation",
        "appsync:getType",
        "appsync:listApis",
        "appsync:listChannelNamespaces",
        "appsync:listDataSources",
        "appsync:listDomainNames",
        "appsync:listFunctions",
```

```
        "appsync:listGraphqlApis",
        "appsync:listResolvers",
        "appsync:listResolversByFunction",
        "appsync:listSourceApiAssociations",
        "appsync:listTypes",
        "appsync:listTypesByAssociation",
        "aps:describeAlertManagerDefinition",
        "aps:describeRuleGroupsNamespace",
        "aps:describeScraper",
        "aps:describeWorkspace",
        "aps:listRuleGroupsNamespaces",
        "aps:listScrapers",
        "aps:listWorkspaces",
        "athena:batchGetNamedQuery",
        "athena:batchGetQueryExecution",
        "athena:getCalculationExecution",
        "athena:getCalculationExecutionStatus",
        "athena:getCapacityAssignmentConfiguration",
        "athena:getCapacityReservation",
        "athena:getDataCatalog",
        "athena:getNamedQuery",
        "athena:getNotebookMetadata",
        "athena:getQueryExecution",
        "athena:getQueryRuntimeStatistics",
        "athena:getSession",
        "athena:getSessionStatus",
        "athena:getWorkGroup",
        "athena:listApplicationDPUSizes",
        "athena:listCalculationExecutions",
        "athena:listCapacityReservations",
        "athena:listDataCatalogs",
        "athena:listEngineVersions",
        "athena:listExecutors",
        "athena:listNamedQueries",
        "athena:listNotebookMetadata",
        "athena:listNotebookSessions",
        "athena:listQueryExecutions",
        "athena:listSessions",
        "athena:listTagsForResource",
        "athena:listWorkGroups",
        "auditmanager:getAccountStatus",
        "auditmanager:getDelegations",
        "auditmanager:listAssessmentFrameworks",
        "auditmanager:listAssessmentReports",
```

```
        "auditmanager:listAssessments",
        "auditmanager:listControls",
        "auditmanager:listKeywordsForDataSource",
        "auditmanager:listNotifications",
        "autoscaling-plans:describeScalingPlanResources",
        "autoscaling-plans:describeScalingPlans",
        "autoscaling-plans:getScalingPlanResourceForecastData",
        "autoscaling:describeAccountLimits",
        "autoscaling:describeAdjustmentTypes",
        "autoscaling:describeAutoScalingGroups",
        "autoscaling:describeAutoScalingInstances",
        "autoscaling:describeAutoScalingNotificationTypes",
        "autoscaling:describeInstanceRefreshes",
        "autoscaling:describeLaunchConfigurations",
        "autoscaling:describeLifecycleHooks",
        "autoscaling:describeLifecycleHookTypes",
        "autoscaling:describeLoadBalancers",
        "autoscaling:describeLoadBalancerTargetGroups",
        "autoscaling:describeMetricCollectionTypes",
        "autoscaling:describeNotificationConfigurations",
        "autoscaling:describePolicies",
        "autoscaling:describeScalingActivities",
        "autoscaling:describeScalingProcessTypes",
        "autoscaling:describeScheduledActions",
        "autoscaling:describeTags",
        "autoscaling:describeTerminationPolicyTypes",
        "autoscaling:describeTrafficSources",
        "autoscaling:describeWarmPool",
        "backup-gateway:getBandwidthRateLimitSchedule",
        "backup-gateway:getGateway",
        "backup-gateway:getHypervisor",
        "backup-gateway:getHypervisorPropertyMappings",
        "backup-gateway:getVirtualMachine",
        "backup-gateway:listGateways",
        "backup-gateway:listHypervisors",
        "backup-gateway:listVirtualMachines",
        "backup-search:listSearchJobBackups",
        "backup-search:listSearchJobs",
        "backup:describeBackupJob",
        "backup:describeBackupVault",
        "backup:describeCopyJob",
        "backup:describeFramework",
        "backup:describeGlobalSettings",
        "backup:describeProtectedResource",
```

```
        "backup:describeRecoveryPoint",
        "backup:describeRegionSettings",
        "backup:describeReportJob",
        "backup:describeReportPlan",
        "backup:describeRestoreJob",
        "backup:getBackupPlan",
        "backup:getBackupPlanFromJSON",
        "backup:getBackupPlanFromTemplate",
        "backup:getBackupSelection",
        "backup:getBackupVaultAccessPolicy",
        "backup:getBackupVaultNotifications",
        "backup:getLegalHold",
        "backup:getRecoveryPointRestoreMetadata",
        "backup:getRecoveryPointIndexDetails",
        "backup:getRestoreJobMetadata",
        "backup:getRestoreTestingInferredMetadata",
        "backup:getRestoreTestingPlan",
        "backup:getRestoreTestingSelection",
        "backup:getSupportedResourceTypes",
        "backup:listBackupJobs",
        "backup:listBackupPlans",
        "backup:listBackupPlanTemplates",
        "backup:listBackupPlanVersions",
        "backup:listBackupSelections",
        "backup:listBackupVaults",
        "backup:listCopyJobs",
        "backup:listFrameworks",
        "backup:listIndexedRecoveryPoints",
        "backup:listLegalHolds",
        "backup:listProtectedResources",
        "backup:listRecoveryPointsByBackupVault",
        "backup:listRecoveryPointsByLegalHold",
        "backup:listRecoveryPointsByResource",
        "backup:listReportJobs",
        "backup:listReportPlans",
        "backup:listRestoreJobs",
        "backup:listRestoreJobsByProtectedResource",
        "backup:listRestoreTestingPlans",
        "backup:listRestoreTestingSelections",
        "backup:listTags",
        "batch:describeComputeEnvironments",
        "batch:describeJobDefinitions",
        "batch:describeJobQueues",
        "batch:describeJobs",
```

```
        "batch:describeSchedulingPolicies",
        "batch:listJobs",
        "bedrock:getAgent",
        "bedrock:getAgentActionGroup",
        "bedrock:getAgentAlias",
        "bedrock:getAgentKnowledgeBase",
        "bedrock:getAgentVersion",
        "bedrock:getCustomModel",
        "bedrock:getDataSource",
        "bedrock:getEvaluationJob",
        "bedrock:getFlow",
        "bedrock:getFlowAlias",
        "bedrock:getFlowVersion",
        "bedrock:getFoundationModel",
        "bedrock:getGuardrail",
        "bedrock:getImportedModel",
        "bedrock:getInferenceProfile",
        "bedrock:getIngestionJob",
        "bedrock:getKnowledgeBase",
        "bedrock:getMarketplaceModelEndpoint",
        "bedrock:getModelCopyJob",
        "bedrock:getModelCustomizationJob",
        "bedrock:getModelImportJob",
        "bedrock:getModelInvocationJob",
        "bedrock:getModelInvocationLoggingConfiguration",
        "bedrock:getPrompt",
        "bedrock:getPromptRouter",
        "bedrock:getProvisionedModelThroughput",
        "bedrock:listAgentActionGroups",
        "bedrock:listAgentAliases",
        "bedrock:listAgentKnowledgeBases",
        "bedrock:listAgents",
        "bedrock:listAgentVersions",
        "bedrock:listCustomModels",
        "bedrock:listDataSources",
        "bedrock:listEvaluationJobs",
        "bedrock:listFlowAliases",
        "bedrock:listFlows",
        "bedrock:listFlowVersions",
        "bedrock:listFoundationModels",
        "bedrock:listGuardrails",
        "bedrock:listImportedModels",
        "bedrock:listInferenceProfiles",
        "bedrock:listIngestionJobs",
```

```
        "bedrock:listKnowledgeBases",
        "bedrock:listMarketplaceModelEndpoints",
        "bedrock:listModelCopyJobs",
        "bedrock:listModelCustomizationJobs",
        "bedrock:listModelImportJobs",
        "bedrock:listModelInvocationJobs",
        "bedrock:listPromptRouters",
        "bedrock:listPrompts",
        "bedrock:listProvisionedModelThroughputs",
        "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:getCollaborationConfiguredAudienceModelAssociation",
        "cleanrooms:getCollaborationPrivacyBudgetTemplate",
        "cleanrooms:getConfiguredTable",
        "cleanrooms:getConfiguredTableAnalysisRule",
        "cleanrooms:getConfiguredTableAssociation",
        "cleanrooms:getConfiguredAudienceModelAssociation",
        "cleanrooms:getMembership",
        "cleanrooms:getPrivacyBudgetTemplate",
        "cleanrooms:getSchema",
        "cleanrooms:getSchemaAnalysisRule",
        "cleanrooms:listAnalysisTemplates",
        "cleanrooms:listCollaborationAnalysisTemplates",
        "cleanrooms:listCollaborationConfiguredAudienceModelAssociations",
        "cleanrooms:listCollaborationPrivacyBudgetTemplates",
        "cleanrooms:listCollaborationPrivacyBudgets",
        "cleanrooms:listCollaborations",
        "cleanrooms:listConfiguredAudienceModelAssociations",
        "cleanrooms:listConfiguredTableAssociations",
        "cleanrooms:listConfiguredTables",
        "cleanrooms:listMembers",
        "cleanrooms:listMemberships",
        "cleanrooms:listPrivacyBudgetTemplates",
        "cleanrooms:listPrivacyBudgets",
        "cleanrooms:listProtectedQueries",
        "cleanrooms:listSchemas",
        "cleanrooms:previewPrivacyImpact",
        "cloud9:describeEnvironmentMemberships",
        "cloud9:describeEnvironments",
        "cloud9:listEnvironments",
        "clouddirectory:getDirectory",
        "clouddirectory:listDirectories",
        "cloudformation:batchDescribeTypeConfigurations",
```

```
        "cloudformation:describeAccountLimits",
        "cloudformation:describeChangeSet",
        "cloudformation:describeChangeSetHooks",
        "cloudformation:describePublisher",
        "cloudformation:describeStackDriftDetectionStatus",
        "cloudformation:describeStackEvents",
        "cloudformation:describeStackInstance",
        "cloudformation:describeStackResource",
        "cloudformation:describeStackResourceDrifts",
        "cloudformation:describeStackResources",
        "cloudformation:describeStacks",
        "cloudformation:describeStackSet",
        "cloudformation:describeStackSetOperation",
        "cloudformation:describeType",
        "cloudformation:describeTypeRegistration",
        "cloudformation:estimateTemplateCost",
        "cloudformation:getResource",
        "cloudformation:getStackPolicy",
        "cloudformation:getTemplate",
        "cloudformation:getTemplateSummary",
        "cloudformation:listChangeSets",
        "cloudformation:listExports",
        "cloudformation:listImports",
        "cloudformation:listResources",
        "cloudformation:listStackInstances",
        "cloudformation:listStackResources",
        "cloudformation:listStacks",
        "cloudformation:listStackSetOperationResults",
        "cloudformation:listStackSetOperations",
        "cloudformation:listStackSets",
        "cloudformation:listTypeRegistrations",
        "cloudformation:listTypes",
        "cloudformation:listTypeVersions",
        "cloudfront:describeFunction",
        "cloudfront:describeKeyValueStore",
        "cloudfront:getAnycastIpList",
        "cloudfront:getCachePolicy",
        "cloudfront:getCachePolicyConfig",
        "cloudfront:getCloudFrontOriginAccessIdentity",
        "cloudfront:getCloudFrontOriginAccessIdentityConfig",
        "cloudfront:getContinuousDeploymentPolicy",
        "cloudfront:getContinuousDeploymentPolicyConfig",
        "cloudfront:getDistribution",
        "cloudfront:getDistributionConfig",
```

```
        "cloudfront:getInvalidation",
        "cloudfront:getKeyGroup",
        "cloudfront:getKeyGroupConfig",
        "cloudfront:getMonitoringSubscription",
        "cloudfront:getOriginAccessControl",
        "cloudfront:getOriginAccessControlConfig",
        "cloudfront:getOriginRequestPolicy",
        "cloudfront:getOriginRequestPolicyConfig",
        "cloudfront:getPublicKey",
        "cloudfront:getPublicKeyConfig",
        "cloudfront:getRealtimeLogConfig",
        "cloudfront:getResponseHeadersPolicy",
        "cloudfront:getResponseHeadersPolicyConfig",
        "cloudfront:getStreamingDistribution",
        "cloudfront:getStreamingDistributionConfig",
        "cloudfront:getVpcOrigin",
        "cloudfront:listAnycastIpLists",
        "cloudfront:listCachePolicies",
        "cloudfront:listCloudFrontOriginAccessIdentities",
        "cloudfront:listConflictingAliases",
        "cloudfront:listContinuousDeploymentPolicies",
        "cloudfront:listDistributions",
        "cloudfront:listDistributionsByAnycastIpListId",
        "cloudfront:listDistributionsByCachePolicyId",
        "cloudfront:listDistributionsByKeyGroup",
        "cloudfront:listDistributionsByOriginRequestPolicyId",
        "cloudfront:listDistributionsByRealtimeLogConfig",
        "cloudfront:listDistributionsByResponseHeadersPolicyId",
        "cloudfront:listDistributionsByVpcOriginId",
        "cloudfront:listDistributionsByWebACLId",
        "cloudfront:listFunctions",
        "cloudfront:listInvalidations",
        "cloudfront:listKeyGroups",
        "cloudfront:listKeyValueStores",
        "cloudfront:listOriginAccessControls",
        "cloudfront:listOriginRequestPolicies",
        "cloudfront:listPublicKeys",
        "cloudfront:listRealtimeLogConfigs",
        "cloudfront:listResponseHeadersPolicies",
        "cloudfront:listStreamingDistributions",
        "cloudfront:listVpcOrigins",
        "cloudhsm:describeBackups",
        "cloudhsm:describeClusters",
        "cloudsearch:describeAnalysisSchemes",
```

```
        "cloudsearch:describeAvailabilityOptions",
        "cloudsearch:describeDomains",
        "cloudsearch:describeExpressions",
        "cloudsearch:describeIndexFields",
        "cloudsearch:describeScalingParameters",
        "cloudsearch:describeServiceAccessPolicies",
        "cloudsearch:describeSuggesters",
        "cloudsearch:listDomainNames",
        "cloudtrail:describeTrails",
        "cloudtrail:getEventSelectors",
        "cloudtrail:getInsightSelectors",
        "cloudtrail:getTrail",
        "cloudtrail:getTrailStatus",
        "cloudtrail:listPublicKeys",
        "cloudtrail:listTags",
        "cloudtrail:listTrails",
        "cloudtrail:lookupEvents",
        "cloudwatch:describeAlarmHistory",
        "cloudwatch:describeAlarms",
        "cloudwatch:describeAlarmsForMetric",
        "cloudwatch:describeAnomalyDetectors",
        "cloudwatch:describeInsightRules",
        "cloudwatch:getDashboard",
        "cloudwatch:getInsightRuleReport",
        "cloudwatch:getMetricData",
        "cloudwatch:getMetricStatistics",
        "cloudwatch:getMetricStream",
        "cloudWatch:getMetricWidgetImage",
        "cloudwatch:listDashboards",
        "cloudwatch:listManagedInsightRules",
        "cloudwatch:listMetrics",
        "cloudwatch:listMetricStreams",
        "codeartifact:describeDomain",
        "codeartifact:describePackageVersion",
        "codeartifact:describeRepository",
        "codeartifact:getDomainPermissionsPolicy",
        "codeartifact:getRepositoryEndpoint",
        "codeartifact:getRepositoryPermissionsPolicy",
        "codeartifact:listDomains",
        "codeartifact:listPackages",
        "codeartifact:listPackageVersionAssets",
        "codeartifact:listPackageVersions",
        "codeartifact:listRepositories",
        "codeartifact:listRepositoriesInDomain",
```

```
            "codebuild:batchGetBuildBatches",
            "codebuild:batchGetBuilds",
            "codebuild:batchGetFleets",
            "codebuild:batchGetProjects",
            "codebuild:listBuildBatches",
            "codebuild:listBuildBatchesForProject",
            "codebuild:listBuilds",
            "codebuild:listBuildsForProject",
            "codebuild:listCuratedEnvironmentImages",
            "codebuild:listFleets",
            "codebuild:listProjects",
            "codebuild:listSourceCredentials",
            "codecommit:batchGetRepositories",
            "codecommit:getBranch",
            "codecommit:getRepository",
            "codecommit:getRepositoryTriggers",
            "codecommit:listBranches",
            "codecommit:listRepositories",
            "codeconnections:getConnection",
            "codeconnections:getHost",
            "codeconnections:getRepositoryLink",
            "codeconnections:getRepositorySyncStatus",
            "codeconnections:getResourceSyncStatus",
            "codeconnections:getSyncBlockerSummary",
            "codeconnections:getSyncConfiguration",
            "codeconnections:listConnections",
            "codeconnections:listHosts",
            "codeconnections:listRepositoryLinks",
            "codeconnections:listRepositorySyncDefinitions",
            "codeconnections:listSyncConfigurations",
            "codedeploy:batchGetApplicationRevisions",
            "codedeploy:batchGetApplications",
            "codedeploy:batchGetDeploymentGroups",
            "codedeploy:batchGetDeploymentInstances",
            "codedeploy:batchGetDeployments",
            "codedeploy:batchGetDeploymentTargets",
            "codedeploy:batchGetOnPremisesInstances",
            "codedeploy:getApplication",
            "codedeploy:getApplicationRevision",
            "codedeploy:getDeployment",
            "codedeploy:getDeploymentConfig",
            "codedeploy:getDeploymentGroup",
            "codedeploy:getDeploymentInstance",
            "codedeploy:getDeploymentTarget",
```

```
        "codedeploy:getOnPremisesInstance",
        "codedeploy:listApplicationRevisions",
        "codedeploy:listApplications",
        "codedeploy:listDeploymentConfigs",
        "codedeploy:listDeploymentGroups",
        "codedeploy:listDeploymentInstances",
        "codedeploy:listDeployments",
        "codedeploy:listDeploymentTargets",
        "codedeploy:listGitHubAccountTokenNames",
        "codedeploy:listOnPremisesInstances",
        "codepipeline:getJobDetails",
        "codepipeline:getPipeline",
        "codepipeline:getPipelineExecution",
        "codepipeline:getPipelineState",
        "codepipeline:listActionExecutions",
        "codepipeline:listActionTypes",
        "codepipeline:listPipelineExecutions",
        "codepipeline:listPipelines",
        "codepipeline:listRuleExecutions",
        "codepipeline:listWebhooks",
        "codestar-connections:getConnection",
        "codestar-connections:getHost",
        "codestar-connections:listConnections",
        "codestar-connections:listHosts",
        "codestar:describeProject",
        "codestar:listProjects",
        "codestar:listResources",
        "codestar:listTeamMembers",
        "codestar:listUserProfiles",
        "cognito-identity:describeIdentity",
        "cognito-identity:describeIdentityPool",
        "cognito-identity:getIdentityPoolAnalytics",
        "cognito-identity:getIdentityPoolDailyAnalytics",
        "cognito-identity:getIdentityPoolRoles",
        "cognito-identity:getIdentityProviderDailyAnalytics",
        "cognito-identity:listIdentities",
        "cognito-identity:listIdentityPools",
        "cognito-identity:lookupDeveloperIdentity",
        "cognito-idp:describeIdentityProvider",
        "cognito-idp:describeResourceServer",
        "cognito-idp:describeRiskConfiguration",
        "cognito-idp:describeUserImportJob",
        "cognito-idp:describeUserPool",
        "cognito-idp:describeUserPoolClient",
```

```
        "cognito-idp:describeUserPoolDomain",
        "cognito-idp:getCSVHeader",
        "cognito-idp:getGroup",
        "cognito-idp:getLogDeliveryConfiguration",
        "cognito-idp:getUICustomization",
        "cognito-idp:getUserPoolMfaConfig",
        "cognito-idp:listGroups",
        "cognito-idp:listIdentityProviders",
        "cognito-idp:listResourceServers",
        "cognito-idp:listUserImportJobs",
        "cognito-idp:listUserPoolClients",
        "cognito-idp:listUserPools",
        "cognito-sync:describeDataset",
        "cognito-sync:describeIdentityPoolUsage",
        "cognito-sync:describeIdentityUsage",
        "cognito-sync:getCognitoEvents",
        "cognito-sync:getIdentityPoolConfiguration",
        "cognito-sync:listDatasets",
        "cognito-sync:listIdentityPoolUsage",
        "comprehend:describeDocumentClassificationJob",
        "comprehend:describeDocumentClassifier",
        "comprehend:describeDominantLanguageDetectionJob",
        "comprehend:describeEndpoint",
        "comprehend:describeEntitiesDetectionJob",
        "comprehend:describeEntityRecognizer",
        "comprehend:describeEventsDetectionJob",
        "comprehend:describeFlywheel",
        "comprehend:describeFlywheelIteration",
        "comprehend:describeKeyPhrasesDetectionJob",
        "comprehend:describePiiEntitiesDetectionJob",
        "comprehend:describeSentimentDetectionJob",
        "comprehend:describeTargetedSentimentDetectionJob",
        "comprehend:describeTopicsDetectionJob",
        "comprehend:listDocumentClassificationJobs",
        "comprehend:listDocumentClassifiers",
        "comprehend:listDominantLanguageDetectionJobs",
        "comprehend:listEndpoints",
        "comprehend:listEntitiesDetectionJobs",
        "comprehend:listEntityRecognizers",
        "comprehend:listEventsDetectionJobs",
        "comprehend:listFlywheelIterationHistory",
        "comprehend:listFlywheels",
        "comprehend:listKeyPhrasesDetectionJobs",
        "comprehend:listPiiEntitiesDetectionJobs",
```

```
        "comprehend:listSentimentDetectionJobs",
        "comprehend:listTargetedSentimentDetectionJobs",
        "comprehend:listTopicsDetectionJobs",
        "compute-optimizer:getAutoScalingGroupRecommendations",
        "compute-optimizer:getEBSVolumeRecommendations",
        "compute-optimizer:getEC2InstanceRecommendations",
        "compute-optimizer:getEC2RecommendationProjectedMetrics",
        "compute-optimizer:getECSServiceRecommendationProjectedMetrics",
        "compute-optimizer:getECSServiceRecommendations",
        "compute-optimizer:getEnrollmentStatus",
        "compute-optimizer:getIdleRecommendations",
        "compute-optimizer:getRDSDatabaseRecommendationProjectedMetrics",
        "compute-optimizer:getRDSDatabaseRecommendations",
        "compute-optimizer:getRecommendationSummaries",
        "config:batchGetAggregateResourceConfig",
        "config:batchGetResourceConfig",
        "config:describeAggregateComplianceByConfigRules",
        "config:describeAggregationAuthorizations",
        "config:describeComplianceByConfigRule",
        "config:describeComplianceByResource",
        "config:describeConfigRuleEvaluationStatus",
        "config:describeConfigRules",
        "config:describeConfigurationAggregators",
        "config:describeConfigurationAggregatorSourcesStatus",
        "config:describeConfigurationRecorders",
        "config:describeConfigurationRecorderStatus",
        "config:describeConformancePackCompliance",
        "config:describeConformancePacks",
        "config:describeConformancePackStatus",
        "config:describeDeliveryChannels",
        "config:describeDeliveryChannelStatus",
        "config:describeOrganizationConfigRules",
        "config:describeOrganizationConfigRuleStatuses",
        "config:describeOrganizationConformancePacks",
        "config:describeOrganizationConformancePackStatuses",
        "config:describePendingAggregationRequests",
        "config:describeRemediationConfigurations",
        "config:describeRemediationExceptions",
        "config:describeRemediationExecutionStatus",
        "config:describeRetentionConfigurations",
        "config:getAggregateComplianceDetailsByConfigRule",
        "config:getAggregateConfigRuleComplianceSummary",
        "config:getAggregateDiscoveredResourceCounts",
        "config:getAggregateResourceConfig",
```

```
        "config:getComplianceDetailsByConfigRule",
        "config:getComplianceDetailsByResource",
        "config:getComplianceSummaryByConfigRule",
        "config:getComplianceSummaryByResourceType",
        "config:getConformancePackComplianceDetails",
        "config:getConformancePackComplianceSummary",
        "config:getDiscoveredResourceCounts",
        "config:getOrganizationConfigRuleDetailedStatus",
        "config:getOrganizationConformancePackDetailedStatus",
        "config:getResourceConfigHistory",
        "config:listAggregateDiscoveredResources",
        "config:listDiscoveredResources",
        "config:listTagsForResource",
        "config:selectAggregateResourceConfig",
        "config:selectResourceConfig",
        "connect:batchGetFlowAssociation",
        "connect:describeContact",
        "connect:describeInstance",
        "connect:describeInstanceAttribute",
        "connect:describePhoneNumber",
        "connect:describeQueue",
        "connect:describeQuickConnect",
        "connect:describeRoutingProfile",
        "connect:describeUser",
        "connect:describeUserHierarchyStructure",
        "connect:getCurrentMetricData",
        "connect:getMetricData",
        "connect:getMetricDataV2",
        "connect:listContactEvaluations",
        "connect:listEvaluationForms",
        "connect:listEvaluationFormVersions",
        "connect:listPhoneNumbersV2",
        "connect:listQueueQuickConnects",
        "connect:listQueues",
        "connect:listQuickConnects",
        "connect:listRoutingProfileQueues",
        "connect:listRoutingProfiles",
        "connect:listSecurityProfiles",
        "connect:listSecurityProfilePermissions",
        "connect:listUsers",
        "connect:listViews",
        "connect:listViewVersions",
        "connect:searchQueues",
        "connect:searchRoutingProfiles",
```

```
        "connect:searchUsers",
        "controltower:describeAccountFactoryConfig",
        "controltower:describeCoreService",
        "controltower:describeGuardrail",
        "controltower:describeGuardrailForTarget",
        "controltower:describeManagedAccount",
        "controltower:describeSingleSignOn",
        "controltower:getAvailableUpdates",
        "controltower:getHomeRegion",
        "controltower:getLandingZone",
        "controltower:getLandingZoneStatus",
        "controltower:listDirectoryGroups",
        "controltower:listEnabledControls",
        "controltower:listGuardrailsForTarget",
        "controltower:listGuardrailViolations",
        "controltower:listLandingZones",
        "controltower:listManagedAccounts",
        "controltower:listManagedAccountsForGuardrail",
        "controltower:listManagedAccountsForParent",
        "controltower:listManagedOrganizationalUnits",
        "controltower:listManagedOrganizationalUnitsForGuardrail",
        "cost-optimization-hub:getPreferences",
        "cost-optimization-hub:getRecommendation",
        "cost-optimization-hub:listEnrollmentStatuses",
        "cost-optimization-hub:listRecommendations",
        "cost-optimization-hub:listRecommendationSummaries",
        "databrew:describeDataset",
        "databrew:describeJob",
        "databrew:describeProject",
        "databrew:describeRecipe",
        "databrew:listDatasets",
        "databrew:listJobRuns",
        "databrew:listJobs",
        "databrew:listProjects",
        "databrew:listRecipes",
        "databrew:listRecipeVersions",
        "databrew:listTagsForResource",
        "datapipeline:describeObjects",
        "datapipeline:describePipelines",
        "datapipeline:getPipelineDefinition",
        "datapipeline:listPipelines",
        "datapipeline:queryObjects",
        "datasync:describeAgent",
        "datasync:describeLocationAzureBlob",
```

```
        "datasync:describeLocationEfs",
        "datasync:describeLocationFsxLustre",
        "datasync:describeLocationFsxOntap",
        "datasync:describeLocationFsxOpenZfs",
        "datasync:describeLocationFsxWindows",
        "datasync:describeLocationHdfs",
        "datasync:describeLocationNfs",
        "datasync:describeLocationObjectStorage",
        "datasync:describeLocationS3",
        "datasync:describeLocationSmb",
        "datasync:describeTask",
        "datasync:describeTaskExecution",
        "datasync:listAgents",
        "datasync:listLocations",
        "datasync:listTaskExecutions",
        "datasync:listTasks",
        "datazone:getAsset",
        "datazone:getAssetType",
        "datazone:getDataSource",
        "datazone:getDataSourceRun",
        "datazone:getDomain",
        "datazone:getEnvironment",
        "datazone:getEnvironmentBlueprint",
        "datazone:getEnvironmentBlueprintConfiguration",
        "datazone:getEnvironmentProfile",
        "datazone:getFormType",
        "datazone:getGlossary",
        "datazone:getGlossaryTerm",
        "datazone:getGroupProfile",
        "datazone:getListing",
        "datazone:getMetadataGenerationRun",
        "datazone:getProject",
        "datazone:getSubscription",
        "datazone:getSubscriptionGrant",
        "datazone:getSubscriptionRequestDetails",
        "datazone:getSubscriptionTarget",
        "datazone:getUserProfile",
        "datazone:listAssetRevisions",
        "datazone:listDataSourceRunActivities",
        "datazone:listDataSourceRuns",
        "datazone:listDataSources",
        "datazone:listDomains",
        "datazone:listEnvironmentBlueprintConfigurations",
        "datazone:listEnvironmentBlueprints",
```

```
        "datazone:listEnvironmentProfiles",
        "datazone:listEnvironments",
        "datazone:listMetadataGenerationRuns",
        "datazone:listProjectMemberships",
        "datazone:listProjects",
        "datazone:listSubscriptionGrants",
        "datazone:listSubscriptionRequests",
        "datazone:listSubscriptions",
        "datazone:listSubscriptionTargets",
        "datazone:searchGroupProfiles",
        "datazone:searchUserProfiles",
        "dax:describeClusters",
        "dax:describeDefaultParameters",
        "dax:describeEvents",
        "dax:describeParameterGroups",
        "dax:describeParameters",
        "dax:describeSubnetGroups",
        "deadline:listAvailableMeteredProducts",
        "deadline:listBudgets",
        "deadline:listFarmMembers",
        "deadline:listFarms",
        "deadline:listFleetMembers",
        "deadline:listFleets",
        "deadline:listJobMembers",
        "deadline:listJobs",
        "deadline:listLicenseEndpoints",
        "deadline:listMeteredProducts",
        "deadline:listMonitors",
        "deadline:listQueueEnvironments",
        "deadline:listQueueFleetAssociations",
        "deadline:listQueueMembers",
        "deadline:listQueues",
        "deadline:listStorageProfiles",
        "deadline:listWorkers",
        "detective:getMembers",
        "detective:listGraphs",
        "detective:listInvitations",
        "detective:listMembers",
        "devicefarm:getAccountSettings",
        "devicefarm:getDevice",
        "devicefarm:getDevicePool",
        "devicefarm:getDevicePoolCompatibility",
        "devicefarm:getJob",
        "devicefarm:getProject",
```

```
        "devicefarm:getRemoteAccessSession",
        "devicefarm:getRun",
        "devicefarm:getSuite",
        "devicefarm:getTest",
        "devicefarm:getTestGridProject",
        "devicefarm:getTestGridSession",
        "devicefarm:getUpload",
        "devicefarm:listArtifacts",
        "devicefarm:listDevicePools",
        "devicefarm:listDevices",
        "devicefarm:listJobs",
        "devicefarm:listProjects",
        "devicefarm:listRemoteAccessSessions",
        "devicefarm:listRuns",
        "devicefarm:listSamples",
        "devicefarm:listSuites",
        "devicefarm:listTestGridProjects",
        "devicefarm:listTestGridSessionActions",
        "devicefarm:listTestGridSessionArtifacts",
        "devicefarm:listTestGridSessions",
        "devicefarm:listTests",
        "devicefarm:listUniqueProblems",
        "devicefarm:listUploads",
        "directconnect:describeConnectionLoa",
        "directconnect:describeConnections",
        "directconnect:describeConnectionsOnInterconnect",
        "directconnect:describeCustomerMetadata",
        "directconnect:describeDirectConnectGatewayAssociationProposals",
        "directconnect:describeDirectConnectGatewayAssociations",
        "directconnect:describeDirectConnectGatewayAttachments",
        "directconnect:describeDirectConnectGateways",
        "directconnect:describeHostedConnections",
        "directconnect:describeInterconnectLoa",
        "directconnect:describeInterconnects",
        "directconnect:describeLags",
        "directconnect:describeLoa",
        "directconnect:describeLocations",
        "directconnect:describeRouterConfiguration",
        "directconnect:describeVirtualGateways",
        "directconnect:describeVirtualInterfaces",
        "directconnect:listVirtualInterfaceTestHistory",
        "dlm:getLifecyclePolicies",
        "dlm:getLifecyclePolicy",
        "dms:describeAccountAttributes",
```

```
        "dms:describeApplicableIndividualAssessments",
        "dms:describeConnections",
        "dms:describeEndpoints",
        "dms:describeEndpointSettings",
        "dms:describeEndpointTypes",
        "dms:describeEventCategories",
        "dms:describeEvents",
        "dms:describeEventSubscriptions",
        "dms:describeFleetAdvisorCollectors",
        "dms:describeFleetAdvisorDatabases",
        "dms:describeFleetAdvisorLsaAnalysis",
        "dms:describeFleetAdvisorSchemaObjectSummary",
        "dms:describeFleetAdvisorSchemas",
        "dms:describeOrderableReplicationInstances",
        "dms:describePendingMaintenanceActions",
        "dms:describeRefreshSchemasStatus",
        "dms:describeReplicationInstances",
        "dms:describeReplicationInstanceTaskLogs",
        "dms:describeReplicationSubnetGroups",
        "dms:describeReplicationTaskAssessmentResults",
        "dms:describeReplicationTaskAssessmentRuns",
        "dms:describeReplicationTaskIndividualAssessments",
        "dms:describeReplicationTasks",
        "dms:describeSchemas",
        "dms:describeTableStatistics",
        "docdb-elastic:getCluster",
        "docdb-elastic:getClusterSnapshot",
        "docdb-elastic:listClusters",
        "docdb-elastic:listClusterSnapshots",
        "drs:describeJobLogItems",
        "drs:describeJobs",
        "drs:describeLaunchConfigurationTemplates",
        "drs:describeRecoveryInstances",
        "drs:describeRecoverySnapshots",
        "drs:describeReplicationConfigurationTemplates",
        "drs:describeSourceNetworks",
        "drs:describeSourceServers",
        "drs:getLaunchConfiguration",
        "drs:getReplicationConfiguration",
        "drs:listExtensibleSourceServers",
        "drs:listLaunchActions",
        "drs:listStagingAccounts",
        "ds:describeClientAuthenticationSettings",
        "ds:describeConditionalForwarders",
```

```
        "ds:describeDirectories",
        "ds:describeDomainControllers",
        "ds:describeEventTopics",
        "ds:describeHybridADUpdate",
        "ds:describeLDAPSSettings",
        "ds:describeSharedDirectories",
        "ds:describeSnapshots",
        "ds:describeTrusts",
        "ds:getDirectoryLimits",
        "ds:getSnapshotLimits",
        "ds:listIpRoutes",
        "ds:listSchemaExtensions",
        "ds:listTagsForResource",
        "dynamodb:describeBackup",
        "dynamodb:describeContinuousBackups",
        "dynamodb:describeContributorInsights",
        "dynamodb:describeExport",
        "dynamodb:describeGlobalTable",
        "dynamodb:describeGlobalTableSettings",
        "dynamodb:describeImport",
        "dynamodb:describeKinesisStreamingDestination",
        "dynamodb:describeLimits",
        "dynamodb:describeStream",
        "dynamodb:describeTable",
        "dynamodb:describeTableReplicaAutoScaling",
        "dynamodb:describeTimeToLive",
        "dynamodb:getResourcePolicy",
        "dynamodb:listBackups",
        "dynamodb:listContributorInsights",
        "dynamodb:listExports",
        "dynamodb:listGlobalTables",
        "dynamodb:listImports",
        "dynamodb:listStreams",
        "dynamodb:listTables",
        "dynamodb:listTagsOfResource",
        "ec2:describeAccountAttributes",
        "ec2:describeAddresses",
        "ec2:describeAddressesAttribute",
        "ec2:describeAddressTransfers",
        "ec2:describeAggregateIdFormat",
        "ec2:describeAvailabilityZones",
        "ec2:describeBundleTasks",
        "ec2:describeByoipCidrs",
        "ec2:describeCapacityBlockOfferings",
```

```
        "ec2:describeCapacityReservationFleets",
        "ec2:describeCapacityReservations",
        "ec2:describeCarrierGateways",
        "ec2:describeClassicLinkInstances",
        "ec2:describeClientVpnAuthorizationRules",
        "ec2:describeClientVpnConnections",
        "ec2:describeClientVpnEndpoints",
        "ec2:describeClientVpnRoutes",
        "ec2:describeClientVpnTargetNetworks",
        "ec2:describeCoipPools",
        "ec2:describeConversionTasks",
        "ec2:describeCustomerGateways",
        "ec2:describeDhcpOptions",
        "ec2:describeEgressOnlyInternetGateways",
        "ec2:describeExportImageTasks",
        "ec2:describeExportTasks",
        "ec2:describeFastLaunchImages",
        "ec2:describeFastSnapshotRestores",
        "ec2:describeFleetHistory",
        "ec2:describeFleetInstances",
        "ec2:describeFleets",
        "ec2:describeFlowLogs",
        "ec2:describeFpgaImageAttribute",
        "ec2:describeFpgaImages",
        "ec2:describeHostReservationOfferings",
        "ec2:describeHostReservations",
        "ec2:describeHosts",
        "ec2:describeIamInstanceProfileAssociations",
        "ec2:describeIdentityIdFormat",
        "ec2:describeIdFormat",
        "ec2:describeImageAttribute",
        "ec2:describeImages",
        "ec2:describeImportImageTasks",
        "ec2:describeImportSnapshotTasks",
        "ec2:describeInstanceAttribute",
        "ec2:describeInstanceConnectEndpoints",
        "ec2:describeInstanceCreditSpecifications",
        "ec2:describeInstanceEventNotificationAttributes",
        "ec2:describeInstanceEventWindows",
        "ec2:describeInstances",
        "ec2:describeInstanceStatus",
        "ec2:describeInstanceTypeOfferings",
        "ec2:describeInstanceTypes",
        "ec2:describeInternetGateways",
```

```
        "ec2:describeIpamByoasn",
        "ec2:describeIpamExternalResourceVerificationTokens",
        "ec2:describeIpamPools",
        "ec2:describeIpamResourceDiscoveries",
        "ec2:describeIpamResourceDiscoveryAssociations",
        "ec2:describeIpams",
        "ec2:describeIpamScopes",
        "ec2:describeIpv6Pools",
        "ec2:describeKeyPairs",
        "ec2:describeLaunchTemplates",
        "ec2:describeLaunchTemplateVersions",
        "ec2:describeLocalGatewayRouteTables",
        "ec2:describeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
        "ec2:describeLocalGatewayRouteTableVpcAssociations",
        "ec2:describeLocalGateways",
        "ec2:describeLocalGatewayVirtualInterfaceGroups",
        "ec2:describeLocalGatewayVirtualInterfaces",
        "ec2:describeManagedPrefixLists",
        "ec2:describeMovingAddresses",
        "ec2:describeNatGateways",
        "ec2:describeNetworkAcls",
        "ec2:describeNetworkInsightsAccessScopeAnalyses",
        "ec2:describeNetworkInsightsAccessScopes",
        "ec2:describeNetworkInsightsAnalyses",
        "ec2:describeNetworkInsightsPaths",
        "ec2:describeNetworkInterfaceAttribute",
        "ec2:describeNetworkInterfaces",
        "ec2:describePlacementGroups",
        "ec2:describePrefixLists",
        "ec2:describePrincipalIdFormat",
        "ec2:describePublicIpv4Pools",
        "ec2:describeRegions",
        "ec2:describeReplaceRootVolumeTasks",
        "ec2:describeReservedInstances",
        "ec2:describeReservedInstancesListings",
        "ec2:describeReservedInstancesModifications",
        "ec2:describeReservedInstancesOfferings",
        "ec2:describeRouteServerEndpoints",
        "ec2:describeRouteServerPeers",
        "ec2:describeRouteServers",
        "ec2:describeRouteTables",
        "ec2:describeScheduledInstanceAvailability",
        "ec2:describeScheduledInstances",
        "ec2:describeSecurityGroupReferences",
```

```
        "ec2:describeSecurityGroupRules",
        "ec2:describeSecurityGroups",
        "ec2:describeServiceLinkVirtualInterfaces",
        "ec2:describeSnapshotAttribute",
        "ec2:describeSnapshots",
        "ec2:describeSnapshotTierStatus",
        "ec2:describeSpotDatafeedSubscription",
        "ec2:describeSpotFleetInstances",
        "ec2:describeSpotFleetRequestHistory",
        "ec2:describeSpotFleetRequests",
        "ec2:describeSpotInstanceRequests",
        "ec2:describeSpotPriceHistory",
        "ec2:describeStaleSecurityGroups",
        "ec2:describeStoreImageTasks",
        "ec2:describeSubnets",
        "ec2:describeTags",
        "ec2:describeTrafficMirrorFilterRules",
        "ec2:describeTrafficMirrorFilters",
        "ec2:describeTrafficMirrorSessions",
        "ec2:describeTrafficMirrorTargets",
        "ec2:describeTransitGatewayAttachments",
        "ec2:describeTransitGatewayConnectPeers",
        "ec2:describeTransitGatewayMulticastDomains",
        "ec2:describeTransitGatewayPeeringAttachments",
        "ec2:describeTransitGatewayPolicyTables",
        "ec2:describeTransitGatewayRouteTableAnnouncements",
        "ec2:describeTransitGatewayRouteTables",
        "ec2:describeTransitGateways",
        "ec2:describeTransitGatewayVpcAttachments",
        "ec2:describeVerifiedAccessEndpoints",
        "ec2:describeVerifiedAccessGroups",
        "ec2:describeVerifiedAccessInstanceLoggingConfigurations",
        "ec2:describeVerifiedAccessInstances",
        "ec2:describeVerifiedAccessTrustProviders",
        "ec2:describeVolumeAttribute",
        "ec2:describeVolumes",
        "ec2:describeVolumesModifications",
        "ec2:describeVolumeStatus",
        "ec2:describeVpcAttribute",
        "ec2:describeVpcBlockPublicAccessExclusions",
        "ec2:describeVpcBlockPublicAccessOptions",
        "ec2:describeVpcClassicLink",
        "ec2:describeVpcClassicLinkDnsSupport",
        "ec2:describeVpcEndpointAssociations",
```

```
        "ec2:describeVpcEndpointConnectionNotifications",
        "ec2:describeVpcEndpointConnections",
        "ec2:describeVpcEndpoints",
        "ec2:describeVpcEndpointServiceConfigurations",
        "ec2:describeVpcEndpointServicePermissions",
        "ec2:describeVpcEndpointServices",
        "ec2:describeVpcPeeringConnections",
        "ec2:describeVpcs",
        "ec2:describeVpnConnections",
        "ec2:describeVpnGateways",
        "ec2:getAssociatedEnclaveCertificateIamRoles",
        "ec2:getAssociatedIpv6PoolCidrs",
        "ec2:getCapacityReservationUsage",
        "ec2:getCoipPoolUsage",
        "ec2:getConsoleOutput",
        "ec2:getConsoleScreenshot",
        "ec2:getDefaultCreditSpecification",
        "ec2:getEbsDefaultKmsKeyId",
        "ec2:getEbsEncryptionByDefault",
        "ec2:getGroupsForCapacityReservation",
        "ec2:getHostReservationPurchasePreview",
        "ec2:getImageBlockPublicAccessState",
        "ec2:getInstanceTypesFromInstanceRequirements",
        "ec2:getIpamAddressHistory",
        "ec2:getIpamDiscoveredAccounts",
        "ec2:getIpamDiscoveredPublicAddresses",
        "ec2:getIpamDiscoveredResourceCidrs",
        "ec2:getIpamPoolAllocations",
        "ec2:getIpamPoolCidrs",
        "ec2:getIpamResourceCidrs",
        "ec2:getLaunchTemplateData",
        "ec2:getManagedPrefixListAssociations",
        "ec2:getManagedPrefixListEntries",
        "ec2:getNetworkInsightsAccessScopeContent",
        "ec2:getReservedInstancesExchangeQuote",
        "ec2:getRouteServerAssociations",
        "ec2:getRouteServerPropagations",
        "ec2:getRouteServerRoutingDatabase",
        "ec2:getSerialConsoleAccessStatus",
        "ec2:getSpotPlacementScores",
        "ec2:getSubnetCidrReservations",
        "ec2:getTransitGatewayMulticastDomainAssociations",
        "ec2:getTransitGatewayPrefixListReferences",
        "ec2:getVerifiedAccessEndpointPolicy",
```

```
        "ec2:getVerifiedAccessGroupPolicy",
        "ec2:listImagesInRecycleBin",
        "ec2:listSnapshotsInRecycleBin",
        "ec2:searchLocalGatewayRoutes",
        "ec2:searchTransitGatewayMulticastGroups",
        "ec2:searchTransitGatewayRoutes",
        "ecr-public:describeImages",
        "ecr-public:describeImageTags",
        "ecr-public:describeRegistries",
        "ecr-public:describeRepositories",
        "ecr-public:getRegistryCatalogData",
        "ecr-public:getRepositoryCatalogData",
        "ecr-public:getRepositoryPolicy",
        "ecr-public:listTagsForResource",
        "ecr:batchCheckLayerAvailability",
        "ecr:batchGetRepositoryScanningConfiguration",
        "ecr:describeImageReplicationStatus",
        "ecr:describeImages",
        "ecr:describeImageScanFindings",
        "ecr:describePullThroughCacheRules",
        "ecr:describeRegistry",
        "ecr:describeRepositories",
        "ecr:getLifecyclePolicy",
        "ecr:getLifecyclePolicyPreview",
        "ecr:getRegistryPolicy",
        "ecr:getRegistryScanningConfiguration",
        "ecr:getRepositoryPolicy",
        "ecr:listImages",
        "ecr:listTagsForResource",
        "ecs:describeCapacityProviders",
        "ecs:describeClusters",
        "ecs:describeContainerInstances",
        "ecs:describeServiceDeployments",
        "ecs:describeServiceRevisions",
        "ecs:describeServices",
        "ecs:describeTaskDefinition",
        "ecs:describeTasks",
        "ecs:describeTaskSets",
        "ecs:getTaskProtection",
        "ecs:listAccountSettings",
        "ecs:listAttributes",
        "ecs:listClusters",
        "ecs:listContainerInstances",
        "ecs:listServiceDeployments",
```

```
        "ecs:listServices",
        "ecs:listServicesByNamespace",
        "ecs:listTagsForResource",
        "ecs:listTaskDefinitionFamilies",
        "ecs:listTaskDefinitions",
        "ecs:listTasks"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AWSSupportActionsGroup2",
      "Action" : [
        "eks:describeAccessEntry",
        "eks:describeAddon",
        "eks:describeAddonConfiguration",
        "eks:describeAddonVersions",
        "eks:describeCluster",
        "eks:describeEksAnywhereSubscription",
        "eks:describeFargateProfile",
        "eks:describeIdentityProviderConfig",
        "eks:describeInsight",
        "eks:describeNodegroup",
        "eks:describePodIdentityAssociation",
        "eks:describeUpdate",
        "eks:listAccessEntries",
        "eks:listAccessPolicies",
        "eks:listAddons",
        "eks:listAssociatedAccessPolicies",
        "eks:listClusters",
        "eks:listEksAnywhereSubscriptions",
        "eks:listFargateProfiles",
        "eks:listIdentityProviderConfigs",
        "eks:listInsights",
        "eks:listNodegroups",
        "eks:listPodIdentityAssociations",
        "eks:listUpdates",
        "elasticache:describeCacheClusters",
        "elasticache:describeCacheEngineVersions",
        "elasticache:describeCacheParameterGroups",
        "elasticache:describeCacheParameters",
        "elasticache:describeCacheSecurityGroups",
```

```
        "elasticache:describeCacheSubnetGroups",
        "elasticache:describeEngineDefaultParameters",
        "elasticache:describeEvents",
        "elasticache:describeGlobalReplicationGroups",
        "elasticache:describeReplicationGroups",
        "elasticache:describeReservedCacheNodes",
        "elasticache:describeReservedCacheNodesOfferings",
        "elasticache:describeServerlessCaches",
        "elasticache:describeServerlessCacheSnapshots",
        "elasticache:describeServiceUpdates",
        "elasticache:describeSnapshots",
        "elasticache:describeUpdateActions",
        "elasticache:describeUserGroups",
        "elasticache:describeUsers",
        "elasticache:listAllowedNodeTypeModifications",
        "elasticache:listTagsForResource",
        "elasticbeanstalk:checkDNSAvailability",
        "elasticbeanstalk:describeAccountAttributes",
        "elasticbeanstalk:describeApplications",
        "elasticbeanstalk:describeApplicationVersions",
        "elasticbeanstalk:describeConfigurationOptions",
        "elasticbeanstalk:describeEnvironmentHealth",
        "elasticbeanstalk:describeEnvironmentManagedActionHistory",
        "elasticbeanstalk:describeEnvironmentManagedActions",
        "elasticbeanstalk:describeEnvironmentResources",
        "elasticbeanstalk:describeEnvironments",
        "elasticbeanstalk:describeEvents",
        "elasticbeanstalk:describeInstancesHealth",
        "elasticbeanstalk:describePlatformVersion",
        "elasticbeanstalk:listAvailableSolutionStacks",
        "elasticbeanstalk:listPlatformBranches",
        "elasticbeanstalk:listPlatformVersions",
        "elasticbeanstalk:validateConfigurationSettings",
        "elasticfilesystem:describeAccessPoints",
        "elasticfilesystem:describeBackupPolicy",
        "elasticfilesystem:describeFileSystemPolicy",
        "elasticfilesystem:describeFileSystems",
        "elasticfilesystem:describeLifecycleConfiguration",
        "elasticfilesystem:describeMountTargets",
        "elasticfilesystem:describeMountTargetSecurityGroups",
        "elasticfilesystem:describeReplicationConfigurations",
        "elasticfilesystem:describeTags",
        "elasticfilesystem:listTagsForResource",
        "elasticloadbalancing:describeAccountLimits",
```

```
        "elasticloadbalancing:describeInstanceHealth",
        "elasticloadbalancing:describeListenerCertificates",
        "elasticloadbalancing:describeListeners",
        "elasticloadbalancing:describeLoadBalancerAttributes",
        "elasticloadbalancing:describeLoadBalancerPolicies",
        "elasticloadbalancing:describeLoadBalancerPolicyTypes",
        "elasticloadbalancing:describeLoadBalancers",
        "elasticloadbalancing:describeRules",
        "elasticloadbalancing:describeSSLPolicies",
        "elasticloadbalancing:describeTags",
        "elasticloadbalancing:describeTargetGroupAttributes",
        "elasticloadbalancing:describeTargetGroups",
        "elasticloadbalancing:describeTargetHealth",
        "elasticloadbalancing:describeTrustStoreAssociations",
        "elasticloadbalancing:describeTrustStoreRevocations",
        "elasticloadbalancing:describeTrustStores",
        "elasticmapreduce:describeCluster",
        "elasticmapreduce:describeNotebookExecution",
        "elasticmapreduce:describePersistentAppUI",
        "elasticmapreduce:describeReleaseLabel",
        "elasticmapreduce:describeSecurityConfiguration",
        "elasticmapreduce:describeStep",
        "elasticmapreduce:describeStudio",
        "elasticmapreduce:getAutoTerminationPolicy",
        "elasticmapreduce:getBlockPublicAccessConfiguration",
        "elasticmapreduce:getManagedScalingPolicy",
        "elasticmapreduce:getStudioSessionMapping",
        "elasticmapreduce:listBootstrapActions",
        "elasticmapreduce:listClusters",
        "elasticmapreduce:listInstanceFleets",
        "elasticmapreduce:listInstanceGroups",
        "elasticmapreduce:listInstances",
        "elasticmapreduce:listNotebookExecutions",
        "elasticmapreduce:listReleaseLabels",
        "elasticmapreduce:listSecurityConfigurations",
        "elasticmapreduce:listSteps",
        "elasticmapreduce:listStudios",
        "elasticmapreduce:listStudioSessionMappings",
        "elasticmapreduce:listSupportedInstanceTypes",
        "elastictranscoder:listJobsByPipeline",
        "elastictranscoder:listJobsByStatus",
        "elastictranscoder:listPipelines",
        "elastictranscoder:listPresets",
        "elastictranscoder:readPipeline",
```

```
        "elastictranscoder:readPreset",
        "emr-containers:describeJobRun",
        "emr-containers:describeJobTemplate",
        "emr-containers:describeManagedEndpoint",
        "emr-containers:describeVirtualCluster",
        "emr-containers:listJobRuns",
        "emr-containers:listJobTemplates",
        "emr-containers:listManagedEndpoints",
        "emr-containers:listVirtualClusters",
        "emr-serverless:getApplication",
        "emr-serverless:getJobRun",
        "emr-serverless:listApplications",
        "es:describeDomain",
        "es:describeDomainAutoTunes",
        "es:describeDomainChangeProgress",
        "es:describeDomainConfig",
        "es:describeDomainHealth",
        "es:describeDomainNodes",
        "es:describeDomains",
        "es:describeDryRunProgress",
        "es:describeElasticsearchDomain",
        "es:describeElasticsearchDomainConfig",
        "es:describeElasticsearchDomains",
        "es:getDomainMaintenanceStatus",
        "es:describeInboundConnections",
        "es:describeInstanceTypeLimits",
        "es:describeOutboundConnections",
        "es:describePackages",
        "es:describeReservedInstanceOfferings",
        "es:describeReservedInstances",
        "es:describeVpcEndpoints",
        "es:getCompatibleVersions",
        "es:getPackageVersionHistory",
        "es:getUpgradeHistory",
        "es:getUpgradeStatus",
        "es:listDomainMaintenances",
        "es:listDomainNames",
        "es:listDomainsForPackage",
        "es:listInstanceTypeDetails",
        "es:listPackagesForDomain",
        "es:listScheduledActions",
        "es:listTags",
        "es:listVersions",
        "es:listVpcEndpointAccess",
```

```
        "es:listVpcEndpoints",
        "es:listVpcEndpointsForDomain",
        "events:describeApiDestination",
        "events:describeArchive",
        "events:describeConnection",
        "events:describeEndpoint",
        "events:describeEventBus",
        "events:describeEventSource",
        "events:describePartnerEventSource",
        "events:describeReplay",
        "events:describeRule",
        "events:listApiDestinations",
        "events:listArchives",
        "events:listConnections",
        "events:listEndpoints",
        "events:listEventBuses",
        "events:listEventSources",
        "events:listPartnerEventSourceAccounts",
        "events:listPartnerEventSources",
        "events:listReplays",
        "events:listRuleNamesByTarget",
        "events:listRules",
        "events:listTargetsByRule",
        "events:testEventPattern",
        "evidently:getExperiment",
        "evidently:getFeature",
        "evidently:getLaunch",
        "evidently:getProject",
        "evidently:getSegment",
        "evidently:listExperiments",
        "evidently:listFeatures",
        "evidently:listLaunches",
        "evidently:listProjects",
        "evidently:listSegmentReferences",
        "evidently:listSegments",
        "firehose:describeDeliveryStream",
        "firehose:listDeliveryStreams",
        "fis:getAction",
        "fis:getExperiment",
        "fis:getExperimentTargetAccountConfiguration",
        "fis:getExperimentTemplate",
        "fis:getSafetyLever",
        "fis:getTargetAccountConfiguration",
        "fis:listActions",
```

```
        "fis:listExperimentResolvedTargets",
        "fis:listExperimentTargetAccountConfigurations",
        "fis:listExperiments",
        "fis:listExperimentTemplates",
        "fis:listTargetAccountConfigurations",
        "fms:getAdminAccount",
        "fms:getAdminScope",
        "fms:getAppsList",
        "fms:getComplianceDetail",
        "fms:getNotificationChannel",
        "fms:getProtocolsList",
        "fms:getPolicy",
        "fms:getProtectionStatus",
        "fms:getResourceSet",
        "fms:getThirdPartyFirewallAssociationStatus",
        "fms:getViolationDetails",
        "fms:listAdminAccountsForOrganization",
        "fms:listAdminsManagingAccount",
        "fms:listAppsLists",
        "fms:listComplianceStatus",
        "fms:listDiscoveredResources",
        "fms:listMemberAccounts",
        "fms:listProtocolsLists",
        "fms:listPolicies",
        "fms:listResourceSetResources",
        "fms:listResourceSets",
        "fms:listThirdPartyFirewallFirewallPolicies",
        "forecast:describeDataset",
        "forecast:describeDatasetGroup",
        "forecast:describeDatasetImportJob",
        "forecast:describeForecast",
        "forecast:describeForecastExportJob",
        "forecast:describePredictor",
        "forecast:getAccuracyMetrics",
        "forecast:listDatasetGroups",
        "forecast:listDatasetImportJobs",
        "forecast:listDatasets",
        "forecast:listForecastExportJobs",
        "forecast:listForecasts",
        "forecast:listPredictors",
        "freetier:getFreeTierUsage",
        "fsx:describeBackups",
        "fsx:describeDataRepositoryAssociations",
        "fsx:describeDataRepositoryTasks",
```

```
        "fsx:describeFileCaches",
        "fsx:describeFileSystems",
        "fsx:describeS3AccessPointAttachments",
        "fsx:describeSnapshots",
        "fsx:describeStorageVirtualMachines",
        "fsx:describeVolumes",
        "fsx:listTagsForResource",
        "gamelift:describeAlias",
        "gamelift:describeBuild",
        "gamelift:describeEC2InstanceLimits",
        "gamelift:describeFleetAttributes",
        "gamelift:describeFleetCapacity",
        "gamelift:describeFleetEvents",
        "gamelift:describeFleetLocationAttributes",
        "gamelift:describeFleetLocationCapacity",
        "gamelift:describeFleetLocationUtilization",
        "gamelift:describeFleetPortSettings",
        "gamelift:describeFleetUtilization",
        "gamelift:describeGameServer",
        "gamelift:describeGameServerGroup",
        "gamelift:describeGameSessionDetails",
        "gamelift:describeGameSessionPlacement",
        "gamelift:describeGameSessionQueues",
        "gamelift:describeGameSessions",
        "gamelift:describeInstances",
        "gamelift:describeMatchmaking",
        "gamelift:describeMatchmakingConfigurations",
        "gamelift:describeMatchmakingRuleSets",
        "gamelift:describePlayerSessions",
        "gamelift:describeRuntimeConfiguration",
        "gamelift:describeScalingPolicies",
        "gamelift:describeScript",
        "gamelift:listAliases",
        "gamelift:listBuilds",
        "gamelift:listFleets",
        "gamelift:listGameServerGroups",
        "gamelift:listGameServers",
        "gamelift:listScripts",
        "gamelift:resolveAlias",
        "geo:calculateRoute",
        "geo:calculateRouteMatrix",
        "geo:describeMap",
        "geo:describePlaceIndex",
        "geo:describeRouteCalculator",
```

```
        "geo:describeTracker",
        "geo:getMapGlyphs",
        "geo:getMapSprites",
        "geo:getMapStyleDescriptor",
        "geo:getMapTile",
        "geo:getPlace",
        "geo:listGeofenceCollections",
        "geo:listMaps",
        "geo:listPlaceIndexes",
        "geo:listRouteCalculators",
        "geo:listTrackerConsumers",
        "geo:searchPlaceIndexForPosition",
        "geo:searchPlaceIndexForSuggestions",
        "geo:searchPlaceIndexForText",
        "geo-maps:getStaticMap",
        "geo-maps:getTile",
        "geo-places:autocomplete",
        "geo-places:geocode",
        "geo-places:getPlace",
        "geo-places:reverseGeocode",
        "geo-places:searchNearby",
        "geo-places:searchText",
        "geo-places:suggest",
        "geo-routes:calculateIsolines",
        "geo-routes:calculateRouteMatrix",
        "geo-routes:calculateRoutes",
        "geo-routes:optimizeWaypoints",
        "geo-routes:snapToRoads",
        "glacier:describeJob",
        "glacier:describeVault",
        "glacier:getDataRetrievalPolicy",
        "glacier:getVaultAccessPolicy",
        "glacier:getVaultLock",
        "glacier:getVaultNotifications",
        "glacier:listJobs",
        "glacier:listTagsForVault",
        "glacier:listVaults",
        "globalaccelerator:describeAccelerator",
        "globalaccelerator:describeAcceleratorAttributes",
        "globalaccelerator:describeCrossAccountAttachment",
        "globalaccelerator:describeCustomRoutingAccelerator",
        "globalaccelerator:describeCustomRoutingAcceleratorAttributes",
        "globalaccelerator:describeCustomRoutingEndpointGroup",
        "globalaccelerator:describeCustomRoutingListener",
```

```
        "globalaccelerator:describeEndpointGroup",
        "globalaccelerator:describeListener",
        "globalaccelerator:listAccelerators",
        "globalaccelerator:listByoipCidrs",
        "globalaccelerator:listCrossAccountAttachments",
        "globalaccelerator:listCrossAccountResourceAccounts",
        "globalaccelerator:listCrossAccountResources",
        "globalaccelerator:listCustomRoutingAccelerators",
        "globalaccelerator:listCustomRoutingEndpointGroups",
        "globalaccelerator:listCustomRoutingListeners",
        "globalaccelerator:listCustomRoutingPortMappings",
        "globalaccelerator:listCustomRoutingPortMappingsByDestination",
        "globalaccelerator:listEndpointGroups",
        "globalaccelerator:listListeners",
        "glue:batchGetBlueprints",
        "glue:batchGetCrawlers",
        "glue:batchGetDevEndpoints",
        "glue:batchGetJobs",
        "glue:batchGetPartition",
        "glue:batchGetTriggers",
        "glue:batchGetWorkflows",
        "glue:checkSchemaVersionValidity",
        "glue:batchGetTableOptimizer",
        "glue:getBlueprint",
        "glue:getBlueprintRun",
        "glue:getBlueprintRuns",
        "glue:getCatalogImportStatus",
        "glue:getClassifier",
        "glue:getClassifiers",
        "glue:getColumnStatisticsForPartition",
        "glue:getColumnStatisticsForTable",
        "glue:getColumnStatisticsTaskRun",
        "glue:getColumnStatisticsTaskRuns",
        "glue:getCrawler",
        "glue:getCrawlerMetrics",
        "glue:getCrawlers",
        "glue:getCustomEntityType",
        "glue:getDatabase",
        "glue:getDatabases",
        "glue:getDataCatalogEncryptionSettings",
        "glue:getDataflowGraph",
        "glue:getDataQualityResult",
        "glue:getDataQualityRuleRecommendationRun",
        "glue:getDataQualityRuleset",
```

```
        "glue:getDataQualityRulesetEvaluationRun",
        "glue:getDevEndpoint",
        "glue:getDevEndpoints",
        "glue:getJob",
        "glue:getJobBookmark",
        "glue:getJobRun",
        "glue:getJobRuns",
        "glue:getJobs",
        "glue:getMapping",
        "glue:getMLTaskRun",
        "glue:getMLTaskRuns",
        "glue:getMLTransform",
        "glue:getMLTransforms",
        "glue:getPartition",
        "glue:getPartitionIndexes",
        "glue:getPartitions",
        "glue:getRegistry",
        "glue:getResourcePolicies",
        "glue:getResourcePolicy",
        "glue:getSchema",
        "glue:getSchemaByDefinition",
        "glue:getSchemaVersion",
        "glue:getSchemaVersionsDiff",
        "glue:getSecurityConfiguration",
        "glue:getSecurityConfigurations",
        "glue:getSession",
        "glue:getStatement",
        "glue:getTable",
        "glue:getTableOptimizer",
        "glue:getTables",
        "glue:getTableVersions",
        "glue:getTrigger",
        "glue:getTriggers",
        "glue:getUserDefinedFunction",
        "glue:getUserDefinedFunctions",
        "glue:getWorkflow",
        "glue:getWorkflowRun",
        "glue:getWorkflowRuns",
        "glue:listColumnStatisticsTaskRuns",
        "glue:listCrawlers",
        "glue:listCrawls",
        "glue:listDataQualityResults",
        "glue:listDataQualityRuleRecommendationRuns",
        "glue:listDataQualityRulesetEvaluationRuns",
```

```
        "glue:listDataQualityRulesets",
        "glue:listDevEndpoints",
        "glue:listMLTransforms",
        "glue:listRegistries",
        "glue:listSchemas",
        "glue:listSchemaVersions",
        "glue:listSessions",
        "glue:listStatements",
        "glue:listTableOptimizerRuns",
        "glue:listTriggers",
        "glue:querySchemaVersionMetadata",
        "glue:getTableVersion",
        "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:describeMalwareScans",
        "guardduty:describePublishingDestination",
        "guardduty:getCoverageStatistics",
        "guardduty:getDetector",
        "guardduty:getFilter",
        "guardduty:getFindings",
        "guardduty:getFindingsStatistics",
        "guardduty:getInvitationsCount",
        "guardduty:getIPSet",
        "guardduty:getMalwareScanSettings",
        "guardduty:getMasterAccount",
        "guardduty:getMemberDetectors",
        "guardduty:getMembers",
        "guardduty:getOrganizationStatistics",
        "guardduty:getRemainingFreeTrialDays",
        "guardduty:getThreatIntelSet",
        "guardduty:listCoverage",
        "guardduty:listDetectors",
        "guardduty:listFilters",
        "guardduty:listFindings",
        "guardduty:listInvitations",
        "guardduty:listIPSets",
        "guardduty:listMembers",
        "guardduty:listThreatIntelSets",
        "health:describeAffectedAccountsForOrganization",
        "health:describeAffectedEntities",
        "health:describeAffectedEntitiesForOrganization",
        "health:describeEntityAggregates",
        "health:describeEntityAggregatesForOrganization",
        "health:describeEventAggregates",
        "health:describeEventDetails",
        "health:describeEventDetailsForOrganization",
        "health:describeEvents",
        "health:describeEventsForOrganization",
        "health:describeEventTypes",
        "health:describeHealthServiceStatusForOrganization",
        "iam:getAccessKeyLastUsed",
        "iam:getAccountAuthorizationDetails",
        "iam:getAccountPasswordPolicy",
```

```
        "iam:getAccountSummary",
        "iam:getContextKeysForCustomPolicy",
        "iam:getContextKeysForPrincipalPolicy",
        "iam:getCredentialReport",
        "iam:getGroup",
        "iam:getGroupPolicy",
        "iam:getInstanceProfile",
        "iam:getLoginProfile",
        "iam:getMFADevice",
        "iam:getOpenIDConnectProvider",
        "iam:getPolicy",
        "iam:getPolicyVersion",
        "iam:getRole",
        "iam:getRolePolicy",
        "iam:getSAMLProvider",
        "iam:getServerCertificate",
        "iam:getServiceLinkedRoleDeletionStatus",
        "iam:getSSHPublicKey",
        "iam:getUser",
        "iam:getUserPolicy",
        "iam:listAccessKeys",
        "iam:listAccountAliases",
        "iam:listAttachedGroupPolicies",
        "iam:listAttachedRolePolicies",
        "iam:listAttachedUserPolicies",
        "iam:listEntitiesForPolicy",
        "iam:listGroupPolicies",
        "iam:listGroups",
        "iam:listGroupsForUser",
        "iam:listInstanceProfiles",
        "iam:listInstanceProfilesForRole",
        "iam:listMFADevices",
        "iam:listOpenIDConnectProviders",
        "iam:listPolicies",
        "iam:listPolicyVersions",
        "iam:listRolePolicies",
        "iam:listRoles",
        "iam:listSAMLProviders",
        "iam:listServerCertificates",
        "iam:listServiceSpecificCredentials",
        "iam:listSigningCertificates",
        "iam:listSSHPublicKeys",
        "iam:listUserPolicies",
        "iam:listUsers",
```

```
        "iam:listVirtualMFADevices",
        "iam:simulateCustomPolicy",
        "iam:simulatePrincipalPolicy",
        "identitystore:describeGroup",
        "identitystore:describeGroupMembership",
        "identitystore:getGroupId",
        "identitystore:getGroupMembershipId",
        "identitystore:getUserId",
        "identitystore:isMemberInGroups",
        "identitystore:listGroupMemberships",
        "identitystore:listGroupMembershipsForMember",
        "identitystore:listGroups",
        "imagebuilder:getComponent",
        "imagebuilder:getComponentPolicy",
        "imagebuilder:getContainerRecipe",
        "imagebuilder:getContainerRecipePolicy",
        "imagebuilder:getDistributionConfiguration",
        "imagebuilder:getImage",
        "imagebuilder:getImagePipeline",
        "imagebuilder:getImagePolicy",
        "imagebuilder:getImageRecipe",
        "imagebuilder:getImageRecipePolicy",
        "imagebuilder:getInfrastructureConfiguration",
        "imagebuilder:getLifecycleExecution",
        "imagebuilder:getLifecyclePolicy",
        "imagebuilder:getWorkflow",
        "imagebuilder:getWorkflowExecution",
        "imagebuilder:getWorkflowStepExecution",
        "imagebuilder:listComponentBuildVersions",
        "imagebuilder:listComponents",
        "imagebuilder:listContainerRecipes",
        "imagebuilder:listDistributionConfigurations",
        "imagebuilder:listImageBuildVersions",
        "imagebuilder:listImagePipelineImages",
        "imagebuilder:listImagePipelines",
        "imagebuilder:listImageRecipes",
        "imagebuilder:listImages",
        "imagebuilder:listImageScanFindingAggregations",
        "imagebuilder:listInfrastructureConfigurations",
        "imagebuilder:listLifecycleExecutionResources",
        "imagebuilder:listLifecycleExecutions",
        "imagebuilder:listLifecyclePolicies",
        "imagebuilder:listTagsForResource",
        "imagebuilder:listWorkflowBuildVersions",
```

```
        "imagebuilder:listWorkflowExecutions",
        "imagebuilder:listWorkflows",
        "imagebuilder:listWaitingWorkflowSteps",
        "imagebuilder:listWorkflowStepExecutions",
        "inspector-scan:scanSbom",
        "inspector:describeAssessmentRuns",
        "inspector:describeAssessmentTargets",
        "inspector:describeAssessmentTemplates",
        "inspector:describeCrossAccountAccessRole",
        "inspector:describeResourceGroups",
        "inspector:describeRulesPackages",
        "inspector:getTelemetryMetadata",
        "inspector:listAssessmentRunAgents",
        "inspector:listAssessmentRuns",
        "inspector:listAssessmentTargets",
        "inspector:listAssessmentTemplates",
        "inspector:listEventSubscriptions",
        "inspector:listRulesPackages",
        "inspector:listTagsForResource",
        "inspector2:batchGetAccountStatus",
        "inspector2:batchGetFreeTrialInfo",
        "inspector2:describeOrganizationConfiguration",
        "inspector2:getConfiguration",
        "inspector2:getDelegatedAdminAccount",
        "inspector2:getEc2DeepInspectionConfiguration",
        "inspector2:getMember",
        "inspector2:getSbomExport",
        "inspector2:listCisScanConfigurations",
        "inspector2:listCisScanResultsAggregatedByChecks",
        "inspector2:listCisScanResultsAggregatedByTargetResource",
        "inspector2:listCisScans",
        "inspector2:listCoverage",
        "inspector2:listDelegatedAdminAccounts",
        "inspector2:listFilters",
        "inspector2:listFindings",
        "inspector2:listMembers",
        "inspector2:listUsageTotals",
        "internetmonitor:getHealthEvent",
        "internetmonitor:getMonitor",
        "internetmonitor:listHealthEvents",
        "internetmonitor:listMonitors",
        "invoicing:listInvoiceSummaries",
        "iot:describeAuthorizer",
        "iot:describeCACertificate",
```

```
        "iot:describeCertificate",
        "iot:describeDefaultAuthorizer",
        "iot:describeDomainConfiguration",
        "iot:describeEndpoint",
        "iot:describeIndex",
        "iot:describeJobExecution",
        "iot:describeThing",
        "iot:describeThingGroup",
        "iot:describeTunnel",
        "iot:getEffectivePolicies",
        "iot:getIndexingConfiguration",
        "iot:getLoggingOptions",
        "iot:getPolicy",
        "iot:getPolicyVersion",
        "iot:getTopicRule",
        "iot:getV2LoggingOptions",
        "iot:listAttachedPolicies",
        "iot:listAuthorizers",
        "iot:listCACertificates",
        "iot:listCertificates",
        "iot:listCertificatesByCA",
        "iot:listCommandExecutions",
        "iot:listCommands",
        "iot:listDomainConfigurations",
        "iot:listJobExecutionsForJob",
        "iot:listJobExecutionsForThing",
        "iot:listJobs",
        "iot:listNamedShadowsForThing",
        "iot:listOutgoingCertificates",
        "iot:listPackages",
        "iot:listPackageVersions",
        "iot:listPolicies",
        "iot:listPolicyPrincipals",
        "iot:listPolicyVersions",
        "iot:listPrincipalPolicies",
        "iot:listPrincipalThings",
        "iot:listRoleAliases",
        "iot:listTargetsForPolicy",
        "iot:listThingGroups",
        "iot:listThingGroupsForThing",
        "iot:listThingPrincipals",
        "iot:listThingRegistrationTasks",
        "iot:listThings",
        "iot:listThingsInThingGroup",
```

```
        "iot:listThingTypes",
        "iot:listTopicRules",
        "iot:listTunnels",
        "iot:listV2LoggingLevels",
        "iotevents:describeDetector",
        "iotevents:describeDetectorModel",
        "iotevents:describeInput",
        "iotevents:describeLoggingOptions",
        "iotevents:listDetectorModels",
        "iotevents:listDetectorModelVersions",
        "iotevents:listDetectors",
        "iotevents:listInputs",
        "iotfleetwise:getCampaign",
        "iotfleetwise:getDecoderManifest",
        "iotfleetwise:getEncryptionConfiguration",
        "iotfleetwise:getFleet",
        "iotfleetwise:getLoggingOptions",
        "iotfleetwise:getModelManifest",
        "iotfleetwise:getRegisterAccountStatus",
        "iotfleetwise:getSignalCatalog",
        "iotfleetwise:getStateTemplate",
        "iotfleetwise:getVehicle",
        "iotfleetwise:getVehicleStatus",
        "iotfleetwise:listCampaigns",
        "iotfleetwise:listDecoderManifestNetworkInterfaces",
        "iotfleetwise:listDecoderManifests",
        "iotfleetwise:listDecoderManifestSignals",
        "iotfleetwise:listFleets",
        "iotfleetwise:listFleetsForVehicle",
        "iotfleetwise:listModelManifestNodes",
        "iotfleetwise:listModelManifests",
        "iotfleetwise:listSignalCatalogNodes",
        "iotfleetwise:listSignalCatalogs",
        "iotfleetwise:listStateTemplates",
        "iotfleetwise:listVehicles",
        "iotfleetwise:listVehiclesInFleet",
        "iotsitewise:describeAccessPolicy",
        "iotsitewise:describeAsset",
        "iotsitewise:describeAssetModel",
        "iotsitewise:describeAssetProperty",
        "iotsitewise:describeDashboard",
        "iotsitewise:describeGateway",
        "iotsitewise:describeGatewayCapabilityConfiguration",
        "iotsitewise:describeLoggingOptions",
```

```
        "iotsitewise:describePortal",
        "iotsitewise:describeProject",
        "iotsitewise:listAccessPolicies",
        "iotsitewise:listAssetModels",
        "iotsitewise:listAssets",
        "iotsitewise:listAssociatedAssets",
        "iotsitewise:listDashboards",
        "iotsitewise:listGateways",
        "iotsitewise:listPortals",
        "iotsitewise:listProjectAssets",
        "iotsitewise:listProjects",
        "iottwinmaker:getComponentType",
        "iottwinmaker:getEntity",
        "iottwinmaker:getPricingPlan",
        "iottwinmaker:getScene",
        "iottwinmaker:getSyncJob",
        "iottwinmaker:getWorkspace",
        "iottwinmaker:listComponentTypes",
        "iottwinmaker:listEntities",
        "iottwinmaker:listScenes",
        "iottwinmaker:listSyncJobs",
        "iottwinmaker:listSyncResources",
        "iottwinmaker:listWorkspaces",
        "iotwireless:getDestination",
        "iotwireless:getDeviceProfile",
        "iotwireless:getPartnerAccount",
        "iotwireless:getServiceEndpoint",
        "iotwireless:getServiceProfile",
        "iotwireless:getWirelessDevice",
        "iotwireless:getWirelessDeviceStatistics",
        "iotwireless:getWirelessGateway",
        "iotwireless:getWirelessGatewayCertificate",
        "iotwireless:getWirelessGatewayFirmwareInformation",
        "iotwireless:getWirelessGatewayStatistics",
        "iotwireless:getWirelessGatewayTask",
        "iotwireless:getWirelessGatewayTaskDefinition",
        "iotwireless:listDestinations",
        "iotwireless:listDeviceProfiles",
        "iotwireless:listPartnerAccounts",
        "iotwireless:listServiceProfiles",
        "iotwireless:listTagsForResource",
        "iotwireless:listWirelessDevices",
        "iotwireless:listWirelessGateways",
        "iotwireless:listWirelessGatewayTaskDefinitions",
```

```
        "ivs:getChannel",
        "ivs:getRecordingConfiguration",
        "ivs:getStream",
        "ivs:getStreamSession",
        "ivs:listChannels",
        "ivs:listPlaybackKeyPairs",
        "ivs:listRecordingConfigurations",
        "ivs:listStreamKeys",
        "ivs:listStreams",
        "ivs:listStreamSessions",
        "kafka:describeCluster",
        "kafka:describeClusterOperation",
        "kafka:describeClusterOperationV2",
        "kafka:describeClusterV2",
        "kafka:describeConfiguration",
        "kafka:describeConfigurationRevision",
        "kafka:describeReplicator",
        "kafka:describeVpcConnection",
        "kafka:getBootstrapBrokers",
        "kafka:getClusterPolicy",
        "kafka:listClientVpcConnections",
        "kafka:listClusterOperations",
        "kafka:listClusterOperationsV2",
        "kafka:listClusters",
        "kafka:listClustersV2",
        "kafka:listConfigurationRevisions",
        "kafka:listConfigurations",
        "kafka:listNodes",
        "kafka:listReplicators",
        "kafka:listScramSecrets",
        "kafka:listVpcConnections",
        "kafkaconnect:describeConnector",
        "kafkaconnect:describeCustomPlugin",
        "kafkaconnect:describeWorkerConfiguration",
        "kafkaconnect:listConnectors",
        "kafkaconnect:listCustomPlugins",
        "kafkaconnect:listWorkerConfigurations",
        "kendra:describeDataSource",
        "kendra:describeFaq",
        "kendra:describeIndex",
        "kendra:listDataSources",
        "kendra:listFaqs",
        "kendra:listIndices",
        "kinesis:describeStream",
```

```
        "kinesis:describeStreamConsumer",
        "kinesis:describeStreamSummary",
        "kinesis:listShards",
        "kinesis:listStreamConsumers",
        "kinesis:listStreams",
        "kinesis:listTagsForStream",
        "kinesisanalytics:describeApplication",
        "kinesisanalytics:describeApplicationOperation",
        "kinesisanalytics:describeApplicationSnapshot",
        "kinesisanalytics:listApplicationOperations",
        "kinesisanalytics:listApplications",
        "kinesisanalytics:listApplicationSnapshots",
        "kinesisanalytics:listApplicationVersions",
        "kinesisvideo:describeImageGenerationConfiguration",
        "kinesisvideo: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",
        "lakeformation:describeLakeFormationIdentityCenterConfiguration",
        "lakeformation:describeResource",
        "lakeformation:describeTransaction",
        "lakeformation:getDataLakePrincipal",
        "lakeformation:getDataLakeSettings",
        "lakeformation:getEffectivePermissionsForPath",
        "lakeformation:getLFTag",
        "lakeformation:getLFTagExpression",
        "lakeformation:getQueryState",
        "lakeformation:getQueryStatistics",
        "lakeformation:getResourceLFTags",
        "lakeformation:listLFTagExpressions",
        "lakeformation:listLFTags",
```

```
        "lakeformation:listLakeFormationOptIns",
        "lakeformation:listPermissions",
        "lakeformation:listResources",
        "lakeformation:searchDatabasesByLFTags",
        "lakeformation:searchTablesByLFTags",
        "lambda:getAccountSettings",
        "lambda:getAlias",
        "lambda:getCodeSigningConfig",
        "lambda:getEventSourceMapping",
        "lambda:getFunction",
        "lambda:getFunctionCodeSigningConfig",
        "lambda:getFunctionConcurrency",
        "lambda:getFunctionConfiguration",
        "lambda:getFunctionEventInvokeConfig",
        "lambda:getFunctionRecursionConfig",
        "lambda:getFunctionUrlConfig",
        "lambda:getLayerVersion",
        "lambda:getLayerVersionPolicy",
        "lambda:getPolicy",
        "lambda:getProvisionedConcurrencyConfig",
        "lambda:getRuntimeManagementConfig",
        "lambda:listAliases",
        "lambda:listCodeSigningConfigs",
        "lambda:listEventSourceMappings",
        "lambda:listFunctionEventInvokeConfigs",
        "lambda:listFunctions",
        "lambda:listFunctionsByCodeSigningConfig",
        "lambda:listFunctionUrlConfigs",
        "lambda:listLayers",
        "lambda:listLayerVersions",
        "lambda:listProvisionedConcurrencyConfigs",
        "lambda:listTags",
        "lambda:listVersionsByFunction",
        "launchwizard:describeProvisionedApp",
        "launchwizard:describeProvisioningEvents",
        "launchwizard:listDeploymentEvents",
        "launchwizard:listDeployments",
        "launchwizard:listProvisionedApps",
        "lex:describeBot",
        "lex:describeBotAlias",
        "lex:describeBotLocale",
        "lex:describeBotRecommendation",
        "lex:describeBotVersion",
        "lex:describeCustomVocabularyMetadata",
```

```
        "lex:describeExport",
        "lex:describeImport",
        "lex:describeIntent",
        "lex:describeResourcePolicy",
        "lex:describeSlot",
        "lex:describeSlotType",
        "lex:getBot",
        "lex:getBotAlias",
        "lex:getBotAliases",
        "lex:getBotChannelAssociation",
        "lex:getBotChannelAssociations",
        "lex:getBots",
        "lex:getBotVersions",
        "lex:getBuiltinIntent",
        "lex:getBuiltinIntents",
        "lex:getBuiltinSlotTypes",
        "lex:getIntent",
        "lex:getIntents",
        "lex:getIntentVersions",
        "lex:getSlotType",
        "lex:getSlotTypes",
        "lex:getSlotTypeVersions",
        "lex:listBotAliases",
        "lex:listBotLocales",
        "lex:listBotRecommendations",
        "lex:listBots",
        "lex:listBotVersions",
        "lex:listExports",
        "lex:listImports",
        "lex:listIntents",
        "lex:listRecommendedIntents",
        "lex:listSlots",
        "lex:listSlotTypes",
        "license-manager: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:describeFieldIndexes",
        "logs:describeIndexPolicies",
        "logs:describeLogGroups",
        "logs:describeLogStreams",
        "logs:describeMetricFilters",
        "logs:describeQueries",
        "logs:describeQueryDefinitions",
        "logs:describeResourcePolicies",
        "logs:describeSubscriptionFilters",
        "logs:getDataProtectionPolicy",
        "logs:getDelivery",
        "logs:getDeliveryDestination",
        "logs:getDeliveryDestinationPolicy",
        "logs:getDeliverySource",
        "logs:getIntegration",
        "logs:getLogAnomalyDetector",
        "logs:getLogDelivery",
        "logs:getLogGroupFields",
        "logs:getTransformer",
        "logs:listAnomalies",
        "logs:listIntegrations",
        "logs:listLogAnomalyDetectors",
        "logs:listLogDeliveries",
        "logs:listLogGroupsForQuery",
        "logs:testMetricFilter",
        "lookoutequipment:describeDataIngestionJob",
        "lookoutequipment:describeDataset",
        "lookoutequipment:describeInferenceScheduler",
        "lookoutequipment:describeModel",
        "lookoutequipment:listDataIngestionJobs",
        "lookoutequipment:listDatasets",
        "lookoutequipment:listInferenceExecutions",
        "lookoutequipment:listInferenceSchedulers",
        "lookoutequipment:listModels",
        "lookoutmetrics:describeAlert",
        "lookoutmetrics:describeAnomalyDetectionExecutions",
```

```
        "lookoutmetrics:describeAnomalyDetector",
        "lookoutmetrics:describeMetricSet",
        "lookoutmetrics:getAnomalyGroup",
        "lookoutmetrics:getDataQualityMetrics",
        "lookoutmetrics:getFeedback",
        "lookoutmetrics:getSampleData",
        "lookoutmetrics:listAlerts",
        "lookoutmetrics:listAnomalyDetectors",
        "lookoutmetrics:listAnomalyGroupSummaries",
        "lookoutmetrics:listAnomalyGroupTimeSeries",
        "lookoutmetrics:listMetricSets",
        "lookoutmetrics:listTagsForResource",
        "m2:getApplication",
        "m2:getApplicationVersion",
        "m2:getBatchJobExecution",
        "m2:getDataSetDetails",
        "m2:getDataSetImportTask",
        "m2:getDeployment",
        "m2:getEnvironment",
        "m2:listApplications",
        "m2:listApplicationVersions",
        "m2:listBatchJobDefinitions",
        "m2:listBatchJobExecutions",
        "m2:listDataSetImportHistory",
        "m2:listDataSets",
        "m2:listDeployments",
        "m2:listEngineVersions",
        "m2:listEnvironments",
        "machinelearning:describeBatchPredictions",
        "machinelearning:describeDataSources",
        "machinelearning:describeEvaluations",
        "machinelearning:describeMLModels",
        "machinelearning:getBatchPrediction",
        "machinelearning:getDataSource",
        "machinelearning:getEvaluation",
        "machinelearning:getMLModel",
        "macie2:getClassificationExportConfiguration",
        "macie2:getCustomDataIdentifier",
        "macie2:getFindings",
        "macie2:getFindingStatistics",
        "macie2:listClassificationJobs",
        "macie2:listCustomDataIdentifiers",
        "macie2:listFindings",
        "managedblockchain:getMember",
```

```
        "managedblockchain:getNetwork",
        "managedblockchain:getNode",
        "managedblockchain:listMembers",
        "managedblockchain:listNetworks",
        "managedblockchain:listNodes",
        "mediaconnect:describeFlow",
        "mediaconnect:listEntitlements",
        "mediaconnect:listFlows",
        "mediaconvert:describeEndpoints",
        "mediaconvert:getJob",
        "mediaconvert:getJobTemplate",
        "mediaconvert:getPreset",
        "mediaconvert:getQueue",
        "mediaconvert:listJobs",
        "mediaconvert:listJobTemplates",
        "medialive:describeChannel",
        "medialive:describeInput",
        "medialive:describeInputDevice",
        "medialive:describeInputSecurityGroup",
        "medialive:describeMultiplex",
        "medialive:describeOffering",
        "medialive:describeReservation",
        "medialive:describeSchedule",
        "medialive:getCloudWatchAlarmTemplate",
        "medialive:getCloudWatchAlarmTemplateGroup",
        "medialive:getEventBridgeRuleTemplate",
        "medialive:getEventBridgeRuleTemplateGroup",
        "medialive:getSignalMap",
        "medialive:listChannels",
        "medialive:listCloudWatchAlarmTemplateGroups",
        "medialive:listCloudWatchAlarmTemplates",
        "medialive:listEventBridgeRuleTemplateGroups",
        "medialive:listEventBridgeRuleTemplates",
        "medialive:listInputDevices",
        "medialive:listInputs",
        "medialive:listInputSecurityGroups",
        "medialive:listMultiplexes",
        "medialive:listOfferings",
        "medialive:listReservations",
        "medialive:listSignalMaps",
        "mediapackage:describeChannel",
        "mediapackage:describeOriginEndpoint",
        "mediapackage:listChannels",
        "mediapackage:listOriginEndpoints",
```

```
        "mediastore:describeContainer",
        "mediastore:getContainerPolicy",
        "mediastore:getCorsPolicy",
        "mediastore:listContainers",
        "mediatailor:getPlaybackConfiguration",
        "mediatailor:listPlaybackConfigurations",
        "medical-imaging:getDatastore",
        "medical-imaging:listDatastores",
        "mgn:describeJobLogItems",
        "mgn:describeJobs",
        "mgn:describeLaunchConfigurationTemplates",
        "mgn:describeReplicationConfigurationTemplates",
        "mgn:describeSourceServers",
        "mgn:describeVcenterClients",
        "mgn:getLaunchConfiguration",
        "mgn:getReplicationConfiguration",
        "mgn:listApplications",
        "mgn:listSourceServerActions",
        "mgn:listTemplateActions",
        "mgn:listWaves",
        "mobiletargeting:getAdmChannel",
        "mobiletargeting:getApnsChannel",
        "mobiletargeting:getApnsSandboxChannel",
        "mobiletargeting:getApnsVoipChannel",
        "mobiletargeting:getApnsVoipSandboxChannel",
        "mobiletargeting:getApp",
        "mobiletargeting:getApplicationSettings",
        "mobiletargeting:getApps",
        "mobiletargeting:getBaiduChannel",
        "mobiletargeting:getCampaign",
        "mobiletargeting:getCampaignActivities",
        "mobiletargeting:getCampaigns",
        "mobiletargeting:getCampaignVersion",
        "mobiletargeting:getCampaignVersions",
        "mobiletargeting:getEmailChannel",
        "mobiletargeting:getEndpoint",
        "mobiletargeting:getEventStream",
        "mobiletargeting:getExportJob",
        "mobiletargeting:getExportJobs",
        "mobiletargeting:getGcmChannel",
        "mobiletargeting:getImportJob",
        "mobiletargeting:getImportJobs",
        "mobiletargeting:getJourney",
        "mobiletargeting:getJourneyExecutionActivityMetrics",
```

```
        "mobiletargeting:getJourneyExecutionMetrics",
        "mobiletargeting:getJourneyRunExecutionActivityMetrics",
        "mobiletargeting:getJourneyRunExecutionMetrics",
        "mobiletargeting:getJourneyRuns",
        "mobiletargeting:getSegment",
        "mobiletargeting:getSegmentImportJobs",
        "mobiletargeting:getSegments",
        "mobiletargeting:getSegmentVersion",
        "mobiletargeting:getSegmentVersions",
        "mobiletargeting:getSmsChannel",
        "mobiletargeting:listJourneys",
        "mobiletargeting:phoneNumberValidate",
        "mq:describeBroker",
        "mq:describeConfiguration",
        "mq:describeConfigurationRevision",
        "mq:describeUser",
        "mq:listBrokers",
        "mq:listConfigurationRevisions",
        "mq:listConfigurations",
        "mq:listUsers",
        "network-firewall:describeFirewall",
        "network-firewall:describeFirewallPolicy",
        "network-firewall:describeFlowOperation",
        "network-firewall:describeLoggingConfiguration",
        "network-firewall:describeResourcePolicy",
        "network-firewall:describeRuleGroup",
        "network-firewall:describeRuleGroupMetadata",
        "network-firewall:describeTlsInspectionConfiguration",
        "network-firewall:describeVpcEndpointAssociation",
        "network-firewall:listAnalysisReports",
        "network-firewall:listFirewallPolicies",
        "network-firewall:listFirewalls",
        "network-firewall:listFlowOperationResults",
        "network-firewall:listFlowOperations",
        "network-firewall:listRuleGroups",
        "network-firewall:listTlsInspectionConfigurations",
        "network-firewall:listVpcEndpointAssociations",
        "networkflowmonitor:getMonitor",
        "networkflowmonitor:getScope",
        "networkflowmonitor:listMonitors",
        "networkflowmonitor:listScopes",
        "networkmanager:describeGlobalNetworks",
        "networkmanager:getConnectAttachment",
        "networkmanager:getConnections",
```

```
        "networkmanager:getConnectPeer",
        "networkmanager:getConnectPeerAssociations",
        "networkmanager:getCoreNetwork",
        "networkmanager:getCoreNetworkChangeEvents",
        "networkmanager:getCoreNetworkChangeSet",
        "networkmanager:getCoreNetworkPolicy",
        "networkmanager:getCustomerGatewayAssociations",
        "networkmanager:getDevices",
        "networkmanager:getDirectConnectGatewayAttachment",
        "networkmanager:getLinkAssociations",
        "networkmanager:getLinks",
        "networkmanager:getNetworkResourceCounts",
        "networkmanager:getNetworkResourceRelationships",
        "networkmanager:getNetworkResources",
        "networkmanager:getNetworkRoutes",
        "networkmanager:getNetworkTelemetry",
        "networkmanager:getResourcePolicy",
        "networkmanager:getRouteAnalysis",
        "networkmanager:getSites",
        "networkmanager:getSiteToSiteVpnAttachment",
        "networkmanager:getTransitGatewayConnectPeerAssociations",
        "networkmanager:getTransitGatewayPeering",
        "networkmanager:getTransitGatewayRegistrations",
        "networkmanager:getTransitGatewayRouteTableAttachment",
        "networkmanager:getVpcAttachment",
        "networkmanager:listAttachments",
        "networkmanager:listConnectPeers",
        "networkmanager:listCoreNetworkPolicyVersions",
        "networkmanager:listCoreNetworks",
        "networkmanager:listOrganizationServiceAccessStatus",
        "networkmanager:listPeerings",
        "networkmanager:listTagsForResource",
        "networkmonitor:getMonitor",
        "networkmonitor:getProbe",
        "networkmonitor:listMonitors",
        "notifications-contacts:getEmailContact",
        "notifications-contacts:listEmailContacts",
        "notifications:getEventRule",
        "notifications:getNotificationConfiguration",
        "notifications:getNotificationEvent",
        "notifications:listChannels",
        "notifications:listEventRules",
        "notifications:listNotificationConfigurations",
        "notifications:listNotificationEvents",
```

```
        "notifications:listNotificationHubs"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AWSSupportActionsGroup3",
      "Action" : [
        "oam:getLink",
        "oam:getSink",
        "oam:getSinkPolicy",
        "oam:listAttachedLinks",
        "oam:listLinks",
        "oam:listSinks",
        "observabilityadmin:getTelemetryEvaluationStatus",
        "observabilityadmin:getTelemetryEvaluationStatusForOrganization",
        "observabilityadmin:listResourceTelemetry",
        "observabilityadmin:listResourceTelemetryForOrganization",
        "odb:getOciOnboardingStatus",
        "odb:getOdbNetwork",
        "odb:getOdbPeeringConnection",
        "odb:listOdbNetworks",
        "odb:listOdbPeeringConnections",
        "omics:getAnnotationImportJob",
        "omics:getAnnotationStore",
        "omics:getAnnotationStoreVersion",
        "omics:getReadSetActivationJob",
        "omics:getReadSetExportJob",
        "omics:getReadSetImportJob",
        "omics:getReadSetMetadata",
        "omics:getReference",
        "omics:getReferenceImportJob",
        "omics:getReferenceMetadata",
        "omics:getReferenceStore",
        "omics:getRun",
        "omics:getRunCache",
        "omics:getRunGroup",
        "omics:getRunTask",
        "omics:getSequenceStore",
        "omics:getShare",
        "omics:getVariantImportJob",
        "omics:getVariantStore",
```

```
        "omics:getWorkflow",
        "omics:getWorkflowVersion",
        "omics:listAnnotationImportJobs",
        "omics:listAnnotationStores",
        "omics:listAnnotationStoreVersions",
        "omics:listMultipartReadSetUploads",
        "omics:listReadSetActivationJobs",
        "omics:listReadSetExportJobs",
        "omics:listReadSetImportJobs",
        "omics:listReadSets",
        "omics:listReadSetUploadParts",
        "omics:listReferenceImportJobs",
        "omics:listReferences",
        "omics:listReferenceStores",
        "omics:listRunCaches",
        "omics:listRunGroups",
        "omics:listRuns",
        "omics:listRunTasks",
        "omics:listSequenceStores",
        "omics:listShares",
        "omics:listVariantImportJobs",
        "omics:listVariantStores",
        "omics:listWorkflows",
        "omics:listWorkflowVersions",
        "opsworks-cm:describeAccountAttributes",
        "opsworks-cm:describeBackups",
        "opsworks-cm:describeEvents",
        "opsworks-cm:describeNodeAssociationStatus",
        "opsworks-cm:describeServers",
        "opsworks:describeAgentVersions",
        "opsworks:describeApps",
        "opsworks:describeCommands",
        "opsworks:describeDeployments",
        "opsworks:describeEcsClusters",
        "opsworks:describeElasticIps",
        "opsworks:describeElasticLoadBalancers",
        "opsworks:describeInstances",
        "opsworks:describeLayers",
        "opsworks:describeLoadBasedAutoScaling",
        "opsworks:describeMyUserProfile",
        "opsworks:describePermissions",
        "opsworks:describeRaidArrays",
        "opsworks:describeRdsDbInstances",
        "opsworks:describeServiceErrors",
```

```
        "opsworks:describeStackProvisioningParameters",
        "opsworks:describeStacks",
        "opsworks:describeStackSummary",
        "opsworks:describeTimeBasedAutoScaling",
        "opsworks:describeUserProfiles",
        "opsworks:describeVolumes",
        "opsworks:getHostnameSuggestion",
        "organizations:describeAccount",
        "organizations:describeCreateAccountStatus",
        "organizations:describeEffectivePolicy",
        "organizations:describeHandshake",
        "organizations:describeOrganization",
        "organizations:describeOrganizationalUnit",
        "organizations:describePolicy",
        "organizations:describeResourcePolicy",
        "organizations:listAccounts",
        "organizations:listAccountsForParent",
        "organizations:listAWSServiceAccessForOrganization",
        "organizations:listChildren",
        "organizations:listCreateAccountStatus",
        "organizations:listDelegatedAdministrators",
        "organizations:listDelegatedServicesForAccount",
        "organizations:listHandshakesForAccount",
        "organizations:listHandshakesForOrganization",
        "organizations:listOrganizationalUnitsForParent",
        "organizations:listParents",
        "organizations:listPolicies",
        "organizations:listPoliciesForTarget",
        "organizations:listRoots",
        "organizations:listTagsForResource",
        "organizations:listTargetsForPolicy",
        "osis:getPipeline",
        "osis:getPipelineBlueprint",
        "osis:getPipelineChangeProgress",
        "osis:listPipelineBlueprints",
        "osis:listPipelines",
        "osis:validatePipeline",
        "outposts:getCapacityTask",
        "outposts:getCatalogItem",
        "outposts:getConnection",
        "outposts:getOrder",
        "outposts:getOutpost",
        "outposts:getOutpostInstanceTypes",
        "outposts:getOutpostSupportedInstanceTypes",
```

```
        "outposts:getSite",
        "outposts:listAssets",
        "outposts:listAssetInstances",
        "outposts:listBlockingInstancesForCapacityTask",
        "outposts:listCapacityTasks",
        "outposts:listCatalogItems",
        "outposts:listOrders",
        "outposts:listOutposts",
        "outposts:listSites",
        "pcs:getCluster",
        "pcs:getComputeNodeGroup",
        "pcs:getQueue",
        "pcs:listClusters",
        "pcs:listComputeNodeGroups",
        "pcs:listQueues",
        "personalize:describeAlgorithm",
        "personalize:describeBatchInferenceJob",
        "personalize:describeBatchSegmentJob",
        "personalize:describeCampaign",
        "personalize:describeDataset",
        "personalize:describeDatasetExportJob",
        "personalize:describeDatasetGroup",
        "personalize:describeDatasetImportJob",
        "personalize:describeEventTracker",
        "personalize:describeFeatureTransformation",
        "personalize:describeFilter",
        "personalize:describeRecipe",
        "personalize:describeRecommender",
        "personalize:describeSchema",
        "personalize:describeSolution",
        "personalize:describeSolutionVersion",
        "personalize:getPersonalizedRanking",
        "personalize:getRecommendations",
        "personalize:getSolutionMetrics",
        "personalize:listBatchInferenceJobs",
        "personalize:listBatchSegmentJobs",
        "personalize:listCampaigns",
        "personalize:listDatasetExportJobs",
        "personalize:listDatasetGroups",
        "personalize:listDatasetImportJobs",
        "personalize:listDatasets",
        "personalize:listEventTrackers",
        "personalize:listRecipes",
        "personalize:listRecommenders",
```

```
        "personalize:listSchemas",
        "personalize:listSolutions",
        "personalize:listSolutionVersions",
        "pipes:describePipe",
        "pipes:listPipes",
        "pipes:listTagsForResource",
        "polly:describeVoices",
        "polly:getLexicon",
        "polly:listLexicons",
        "pricing:describeServices",
        "pricing:getAttributeValues",
        "pricing:getProducts",
        "private-networks:getDeviceIdentifier",
        "private-networks:getNetwork",
        "private-networks:getNetworkResource",
        "private-networks:listDeviceIdentifiers",
        "private-networks:listNetworkResources",
        "private-networks:listNetworks",
        "qbusiness:getApplication",
        "qbusiness:getDataSource",
        "qbusiness:getIndex",
        "qbusiness:getRetriever",
        "qbusiness:getWebExperience",
        "qbusiness:listApplications",
        "qbusiness:listDataSources",
        "qbusiness:listDataSourceSyncJobs",
        "qbusiness:listIndices",
        "qbusiness:listRetrievers",
        "qbusiness:listWebExperiences",
        "quicksight:describeAccountCustomization",
        "quicksight:describeAccountSettings",
        "quicksight:describeAccountSubscription",
        "quicksight:describeAnalysis",
        "quicksight:describeAnalysisPermissions",
        "quicksight:describeDashboard",
        "quicksight:describeDashboardPermissions",
        "quicksight:describeDataSet",
        "quicksight:describeDataSetPermissions",
        "quicksight:describeDataSetRefreshProperties",
        "quicksight:describeDataSource",
        "quicksight:describeDataSourcePermissions",
        "quicksight:describeFolder",
        "quicksight:describeFolderPermissions",
        "quicksight:describeFolderResolvedPermissions",
```

```
        "quicksight:describeGroup",
        "quicksight:describeGroupMembership",
        "quicksight:describeIAMPolicyAssignment",
        "quicksight:describeIngestion",
        "quicksight:describeIpRestriction",
        "quicksight:describeNamespace",
        "quicksight:describeRefreshSchedule",
        "quicksight:describeTemplate",
        "quicksight:describeTemplateAlias",
        "quicksight:describeTemplatePermissions",
        "quicksight:describeTheme",
        "quicksight:describeThemeAlias",
        "quicksight:describeThemePermissions",
        "quicksight:describeTopic",
        "quicksight:describeTopicPermissions",
        "quicksight:describeTopicRefresh",
        "quicksight:describeTopicRefreshSchedule",
        "quicksight:describeUser",
        "quicksight:describeVPCConnection",
        "quicksight:listAnalyses",
        "quicksight:listDashboards",
        "quicksight:listDashboardVersions",
        "quicksight:listDataSets",
        "quicksight:listDataSources",
        "quicksight:listFolderMembers",
        "quicksight:listFolders",
        "quicksight:listGroupMemberships",
        "quicksight:listGroups",
        "quicksight:listIAMPolicyAssignments",
        "quicksight:listIAMPolicyAssignmentsForUser",
        "quicksight:listIngestions",
        "quicksight:listNamespaces",
        "quicksight:listRefreshSchedules",
        "quicksight:listTemplateAliases",
        "quicksight:listTemplates",
        "quicksight:listTemplateVersions",
        "quicksight:listThemeAliases",
        "quicksight:listThemes",
        "quicksight:listThemeVersions",
        "quicksight:listTopicRefreshSchedules",
        "quicksight:listTopics",
        "quicksight:listUserGroups",
        "quicksight:listUsers",
        "quicksight:listVPCConnections",
```

```
        "quicksight:searchAnalyses",
        "quicksight:searchDashboards",
        "quicksight:searchDataSets",
        "quicksight:searchDataSources",
        "quicksight:searchFolders",
        "quicksight:searchGroups",
        "ram:getPermission",
        "ram:getResourceShareAssociations",
        "ram:getResourceShareInvitations",
        "ram:getResourceShares",
        "ram:listPendingInvitationResources",
        "ram:listPrincipals",
        "ram:listResources",
        "ram:listResourceSharePermissions",
        "rbin:getRule",
        "rbin:listRules",
        "rds:describeAccountAttributes",
        "rds:describeBlueGreenDeployments",
        "rds:describeCertificates",
        "rds: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-serverless:getCustomDomainAssociation",
        "redshift-serverless:getEndpointAccess",
        "redshift-serverless:getNamespace",
        "redshift-serverless:getRecoveryPoint",
        "redshift-serverless:getScheduledAction",
        "redshift-serverless:getSnapshot",
        "redshift-serverless:getTableRestoreStatus",
        "redshift-serverless:getUsageLimit",
        "redshift-serverless:getWorkgroup",
        "redshift-serverless:listCustomDomainAssociations",
        "redshift-serverless:listEndpointAccess",
        "redshift-serverless:listNamespaces",
        "redshift-serverless:listRecoveryPoints",
        "redshift-serverless:listSnapshotCopyConfigurations",
        "redshift-serverless:listSnapshots",
        "redshift-serverless:listTableRestoreStatus",
        "redshift-serverless:listUsageLimits",
        "redshift-serverless:listWorkgroups",
        "redshift:describeClusterDbRevisions",
        "redshift:describeClusterParameterGroups",
        "redshift:describeClusterParameters",
        "redshift:describeClusters",
        "redshift:describeClusterSecurityGroups",
        "redshift:describeClusterSnapshots",
        "redshift:describeClusterSubnetGroups",
        "redshift:describeClusterTracks",
        "redshift:describeClusterVersions",
        "redshift:describeCustomDomainAssociations",
        "redshift:describeDataShares",
        "redshift:describeDataSharesForConsumer",
        "redshift:describeDataSharesForProducer",
        "redshift:describeDefaultClusterParameters",
        "redshift:describeEndpointAccess",
        "redshift:describeEndpointAuthorization",
        "redshift:describeEventCategories",
```

```
        "redshift:describeEvents",
        "redshift:describeEventSubscriptions",
        "redshift:describeHsmClientCertificates",
        "redshift:describeHsmConfigurations",
        "redshift:describeInboundIntegrations",
        "redshift:describeLoggingStatus",
        "redshift:describeNodeConfigurationOptions",
        "redshift:describeOrderableClusterOptions",
        "redshift:describeRedshiftIdcApplications",
        "redshift:describeReservedNodeOfferings",
        "redshift:describeReservedNodes",
        "redshift:describeResize",
        "redshift:describeSnapshotCopyGrants",
        "redshift:describeSnapshotSchedules",
        "redshift:describeStorage",
        "redshift:describeTableRestoreStatus",
        "redshift:describeTags",
        "redshift:describeUsageLimits",
        "rekognition:listCollections",
        "rekognition:listFaces",
        "resiliencehub:describeApp",
        "resiliencehub:describeAppAssessment",
        "resiliencehub:describeAppVersion",
        "resiliencehub:describeAppVersionAppComponent",
        "resiliencehub:describeAppVersionResource",
        "resiliencehub:describeAppVersionResourcesResolutionStatus",
        "resiliencehub:describeAppVersionTemplate",
        "resiliencehub:describeDraftAppVersionResourcesImportStatus",
        "resiliencehub:describeResiliencyPolicy",
        "resiliencehub:describeResourceGroupingRecommendationTask",
        "resiliencehub:listAlarmRecommendations",
        "resiliencehub:listAppAssessmentComplianceDrifts",
        "resiliencehub:listAppAssessmentResourceDrifts",
        "resiliencehub:listAppAssessments",
        "resiliencehub:listAppComponentCompliances",
        "resiliencehub:listAppComponentRecommendations",
        "resiliencehub:listAppInputSources",
        "resiliencehub:listApps",
        "resiliencehub:listAppVersionAppComponents",
        "resiliencehub:listAppVersionResourceMappings",
        "resiliencehub:listAppVersionResources",
        "resiliencehub:listAppVersions",
        "resiliencehub:listRecommendationTemplates",
        "resiliencehub:listResiliencyPolicies",
```

```
        "resiliencehub:listResourceGroupingRecommendations",
        "resiliencehub:listSopRecommendations",
        "resiliencehub:listSuggestedResiliencyPolicies",
        "resiliencehub:listTestRecommendations",
        "resiliencehub:listUnsupportedAppVersionResources",
        "resource-explorer-2:getAccountLevelServiceConfiguration",
        "resource-explorer-2:getIndex",
        "resource-explorer-2:getView",
        "resource-explorer-2:listIndexes",
        "resource-explorer-2:listViews",
        "resource-explorer-2:search",
        "resource-groups:getGroup",
        "resource-groups:getGroupQuery",
        "resource-groups:getTags",
        "resource-groups:listGroupResources",
        "resource-groups:listGroups",
        "resource-groups:searchResources",
        "robomaker:batchDescribeSimulationJob",
        "robomaker:describeDeploymentJob",
        "robomaker:describeFleet",
        "robomaker:describeRobot",
        "robomaker:describeRobotApplication",
        "robomaker:describeSimulationApplication",
        "robomaker:describeSimulationJob",
        "robomaker:listDeploymentJobs",
        "robomaker:listFleets",
        "robomaker:listRobotApplications",
        "robomaker:listRobots",
        "robomaker:listSimulationApplications",
        "robomaker:listSimulationJobs",
        "rolesanywhere:getProfile",
        "rolesanywhere:getTrustAnchor",
        "rolesanywhere:listProfiles",
        "rolesanywhere:listTrustAnchors",
        "route53-recovery-cluster:getRoutingControlState",
        "route53-recovery-cluster:listRoutingControls",
        "route53-recovery-control-config:describeControlPanel",
        "route53-recovery-control-config:describeRoutingControl",
        "route53-recovery-control-config:describeSafetyRule",
        "route53-recovery-control-config:listControlPanels",
        "route53-recovery-control-config:listRoutingControls",
        "route53-recovery-control-config:listSafetyRules",
        "route53-recovery-readiness:getCell",
        "route53-recovery-readiness:getCellReadinessSummary",
```

```
        "route53-recovery-readiness:getReadinessCheck",
        "route53-recovery-readiness:getReadinessCheckResourceStatus",
        "route53-recovery-readiness:getReadinessCheckStatus",
        "route53-recovery-readiness:getRecoveryGroup",
        "route53-recovery-readiness:getRecoveryGroupReadinessSummary",
        "route53-recovery-readiness:listCells",
        "route53-recovery-readiness:listReadinessChecks",
        "route53-recovery-readiness:listRecoveryGroups",
        "route53-recovery-readiness:listResourceSets",
        "route53:getAccountLimit",
        "route53:getChange",
        "route53:getCheckerIpRanges",
        "route53:getDNSSEC",
        "route53:getGeoLocation",
        "route53:getHealthCheck",
        "route53:getHealthCheckCount",
        "route53:getHealthCheckLastFailureReason",
        "route53:getHealthCheckStatus",
        "route53:getHostedZone",
        "route53:getHostedZoneCount",
        "route53:getHostedZoneLimit",
        "route53:getQueryLoggingConfig",
        "route53:getReusableDelegationSet",
        "route53:getTrafficPolicy",
        "route53:getTrafficPolicyInstance",
        "route53:getTrafficPolicyInstanceCount",
        "route53:listCidrBlocks",
        "route53:listCidrCollections",
        "route53:listCidrLocations",
        "route53:listGeoLocations",
        "route53:listHealthChecks",
        "route53:listHostedZones",
        "route53:listHostedZonesByName",
        "route53:listHostedZonesByVpc",
        "route53:listQueryLoggingConfigs",
        "route53:listResourceRecordSets",
        "route53:listReusableDelegationSets",
        "route53:listTrafficPolicies",
        "route53:listTrafficPolicyInstances",
        "route53:listTrafficPolicyInstancesByHostedZone",
        "route53:listTrafficPolicyInstancesByPolicy",
        "route53:listTrafficPolicyVersions",
        "route53:listVPCAssociationAuthorizations",
        "route53domains:checkDomainAvailability",
```

```
        "route53domains:getContactReachabilityStatus",
        "route53domains:getDomainDetail",
        "route53domains:getOperationDetail",
        "route53domains:listDomains",
        "route53domains:listOperations",
        "route53domains:listPrices",
        "route53domains:listTagsForDomain",
        "route53domains:viewBilling",
        "route53profiles:getProfile",
        "route53profiles:getProfileAssociation",
        "route53profiles:getProfileResourceAssociation",
        "route53profiles:listProfileAssociations",
        "route53profiles:listProfileResourceAssociations",
        "route53profiles:listProfiles",
        "route53profiles:listTagsForResource",
        "route53resolver:getFirewallConfig",
        "route53resolver:getFirewallDomainList",
        "route53resolver:getFirewallRuleGroup",
        "route53resolver:getFirewallRuleGroupAssociation",
        "route53resolver:getFirewallRuleGroupPolicy",
        "route53resolver:getOutpostResolver",
        "route53resolver:getResolverDnssecConfig",
        "route53resolver:getResolverQueryLogConfig",
        "route53resolver:getResolverQueryLogConfigAssociation",
        "route53resolver:getResolverQueryLogConfigPolicy",
        "route53resolver:getResolverRule",
        "route53resolver:getResolverRuleAssociation",
        "route53resolver:getResolverRulePolicy",
        "route53resolver:listFirewallConfigs",
        "route53resolver:listFirewallDomainLists",
        "route53resolver:listFirewallDomains",
        "route53resolver:listFirewallRuleGroupAssociations",
        "route53resolver:listFirewallRuleGroups",
        "route53resolver:listFirewallRules",
        "route53resolver:listOutpostResolvers",
        "route53resolver:listResolverConfigs",
        "route53resolver:listResolverDnssecConfigs",
        "route53resolver:listResolverEndpointIpAddresses",
        "route53resolver:listResolverEndpoints",
        "route53resolver:listResolverQueryLogConfigAssociations",
        "route53resolver:listResolverQueryLogConfigs",
        "route53resolver:listResolverRuleAssociations",
        "route53resolver:listResolverRules",
        "route53resolver:listTagsForResource",
```

```
        "rum:batchGetRumMetricDefinitions",
        "rum:getAppMonitor",
        "rum:listAppMonitors",
        "rum:listRumMetricsDestinations",
        "s3-outposts:listEndpoints",
        "s3-outposts:listOutpostsWithS3",
        "s3-outposts:listRegionalBuckets",
        "s3-outposts:listSharedEndpoints",
        "s3:describeJob",
        "s3:describeMultiRegionAccessPointOperation",
        "s3:getAccelerateConfiguration",
        "s3:getAccessGrant",
        "s3:getAccessGrantsInstance",
        "s3:getAccessGrantsInstanceResourcePolicy",
        "s3:getAccessGrantsLocation",
        "s3:getAccessPoint",
        "s3:getAccessPointConfigurationForObjectLambda",
        "s3:getAccessPointForObjectLambda",
        "s3:getAccessPointPolicy",
        "s3:getAccessPointPolicyForObjectLambda",
        "s3:getAccessPointPolicyStatus",
        "s3:getAccessPointPolicyStatusForObjectLambda",
        "s3:getAccountPublicAccessBlock",
        "s3:getAnalyticsConfiguration",
        "s3:getBucketAcl",
        "s3:getBucketCORS",
        "s3:getBucketLocation",
        "s3:getBucketLogging",
        "s3:getBucketNotification",
        "s3:getBucketObjectLockConfiguration",
        "s3:getBucketOwnershipControls",
        "s3:getBucketPolicy",
        "s3:getBucketPolicyStatus",
        "s3:getBucketPublicAccessBlock",
        "s3:getBucketRequestPayment",
        "s3:getBucketVersioning",
        "s3:getBucketWebsite",
        "s3:getEncryptionConfiguration",
        "s3:getIntelligentTieringConfiguration",
        "s3:getInventoryConfiguration",
        "s3:getLifecycleConfiguration",
        "s3:getMetricsConfiguration",
        "s3:getMultiRegionAccessPoint",
        "s3:getMultiRegionAccessPointPolicy",
```

```
        "s3:getMultiRegionAccessPointPolicyStatus",
        "s3:getMultiRegionAccessPointRoutes",
        "s3:getObjectAcl",
        "s3:getObjectLegalHold",
        "s3:getObjectRetention",
        "s3:getReplicationConfiguration",
        "s3:getStorageLensConfiguration",
        "s3:listAccessGrants",
        "s3:listAccessGrantsInstances",
        "s3:listAccessGrantsLocations",
        "s3:listAccessPoints",
        "s3:listAccessPointsForObjectLambda",
        "s3:listAllMyBuckets",
        "s3:listBucket",
        "s3:listBucketMultipartUploads",
        "s3:listBucketVersions",
        "s3:listJobs",
        "s3:listMultipartUploadParts",
        "s3:listMultiRegionAccessPoints",
        "s3:listStorageLensConfigurations",
        "s3express:getBucketPolicy",
        "s3express:listAllMyDirectoryBuckets",
        "s3tables:getNamespace",
        "s3tables:getTable",
        "s3tables:getTableBucket",
        "s3tables:getTableBucketEncryption",
        "s3tables:getTableBucketMaintenanceConfiguration",
        "s3tables:getTableBucketPolicy",
        "s3tables:getTableEncryption",
        "s3tables:getTableMaintenanceConfiguration",
        "s3tables:getTableMaintenanceJobStatus",
        "s3tables:getTableMetadataLocation",
        "s3tables:getTablePolicy",
        "s3tables:listNamespaces",
        "s3tables:listTableBuckets",
        "s3tables:listTables",
        "s3vectors:getIndex",
        "s3vectors:getVectorBucket",
        "s3vectors:getVectorBucketPolicy",
        "s3vectors:listIndexes",
        "s3vectors:listVectorBuckets",
        "sagemaker:describeAction",
        "sagemaker:describeAlgorithm",
        "sagemaker:describeApp",
```

```
        "sagemaker:describeAppImageConfig",
        "sagemaker:describeArtifact",
        "sagemaker:describeAutoMLJob",
        "sagemaker:describeCluster",
        "sagemaker:describeClusterNode",
        "sagemaker:describeCodeRepository",
        "sagemaker:describeCompilationJob",
        "sagemaker:describeContext",
        "sagemaker:describeDataQualityJobDefinition",
        "sagemaker:describeDevice",
        "sagemaker:describeDeviceFleet",
        "sagemaker:describeDomain",
        "sagemaker:describeEdgeDeploymentPlan",
        "sagemaker:describeEdgePackagingJob",
        "sagemaker:describeEndpoint",
        "sagemaker:describeEndpointConfig",
        "sagemaker:describeExperiment",
        "sagemaker:describeFeatureGroup",
        "sagemaker:describeFeatureMetadata",
        "sagemaker:describeFlowDefinition",
        "sagemaker:describeHub",
        "sagemaker:describeHubContent",
        "sagemaker:describeHumanTaskUi",
        "sagemaker:describeHyperParameterTuningJob",
        "sagemaker:describeImage",
        "sagemaker:describeImageVersion",
        "sagemaker:describeInferenceComponent",
        "sagemaker:describeInferenceExperiment",
        "sagemaker:describeInferenceRecommendationsJob",
        "sagemaker:describeLabelingJob",
        "sagemaker:describeMlflowTrackingServer",
        "sagemaker:describeModel",
        "sagemaker:describeModelBiasJobDefinition",
        "sagemaker:describeModelCard",
        "sagemaker:describeModelCardExportJob",
        "sagemaker:describeModelExplainabilityJobDefinition",
        "sagemaker:describeModelPackage",
        "sagemaker:describeModelPackageGroup",
        "sagemaker:describeModelQualityJobDefinition",
        "sagemaker:describeMonitoringSchedule",
        "sagemaker:describeNotebookInstance",
        "sagemaker:describeNotebookInstanceLifecycleConfig",
        "sagemaker:describePipeline",
        "sagemaker:describePipelineDefinitionForExecution",
```

```
        "sagemaker:describePipelineExecution",
        "sagemaker:describePartnerApp",
        "sagemaker:describeProcessingJob",
        "sagemaker:describeProject",
        "sagemaker:describeSpace",
        "sagemaker:describeStudioLifecycleConfig",
        "sagemaker:describeSubscribedWorkteam",
        "sagemaker:describeTrainingJob",
        "sagemaker:describeTransformJob",
        "sagemaker:describeTrial",
        "sagemaker:describeTrialComponent",
        "sagemaker:describeUserProfile",
        "sagemaker:describeWorkforce",
        "sagemaker:describeWorkteam",
        "sagemaker:getDeviceFleetReport",
        "sagemaker:getModelPackageGroupPolicy",
        "sagemaker:getSagemakerServicecatalogPortfolioStatus",
        "sagemaker:listActions",
        "sagemaker:listAlgorithms",
        "sagemaker:listAliases",
        "sagemaker:listAppImageConfigs",
        "sagemaker:listApps",
        "sagemaker:listArtifacts",
        "sagemaker:listAssociations",
        "sagemaker:listAutoMLJobs",
        "sagemaker:listCandidatesForAutoMLJob",
        "sagemaker:listClusterNodes",
        "sagemaker:listClusters",
        "sagemaker:listCodeRepositories",
        "sagemaker:listCompilationJobs",
        "sagemaker:listContexts",
        "sagemaker:listDataQualityJobDefinitions",
        "sagemaker:listDeviceFleets",
        "sagemaker:listDevices",
        "sagemaker:listDomains",
        "sagemaker:listEdgeDeploymentPlans",
        "sagemaker:listEdgePackagingJobs",
        "sagemaker:listEndpointConfigs",
        "sagemaker:listEndpoints",
        "sagemaker:listExperiments",
        "sagemaker:listFeatureGroups",
        "sagemaker:listFlowDefinitions",
        "sagemaker:listHubContents",
        "sagemaker:listHubContentVersions",
```

```
        "sagemaker:listHubs",
        "sagemaker:listHumanTaskUis",
        "sagemaker:listHyperParameterTuningJobs",
        "sagemaker:listImages",
        "sagemaker:listImageVersions",
        "sagemaker:listInferenceComponents",
        "sagemaker:listInferenceExperiments",
        "sagemaker:listInferenceRecommendationsJobs",
        "sagemaker:listInferenceRecommendationsJobSteps",
        "sagemaker:listLabelingJobs",
        "sagemaker:listLabelingJobsForWorkteam",
        "sagemaker:listLineageGroups",
        "sagemaker:listMlflowTrackingServers",
        "sagemaker:listModelBiasJobDefinitions",
        "sagemaker:listModelCardExportJobs",
        "sagemaker:listModelCards",
        "sagemaker:listModelCardVersions",
        "sagemaker:listModelExplainabilityJobDefinitions",
        "sagemaker:listModelMetadata",
        "sagemaker:listModelPackageGroups",
        "sagemaker:listModelPackages",
        "sagemaker:listModelQualityJobDefinitions",
        "sagemaker:listModels",
        "sagemaker:listMonitoringAlertHistory",
        "sagemaker:listMonitoringAlerts",
        "sagemaker:listMonitoringExecutions",
        "sagemaker:listMonitoringSchedules",
        "sagemaker:listNotebookInstanceLifecycleConfigs",
        "sagemaker:listNotebookInstances",
        "sagemaker:listPartnerApps",
        "sagemaker:listPipelineExecutions",
        "sagemaker:listPipelineExecutionSteps",
        "sagemaker:listPipelineParametersForExecution",
        "sagemaker:listPipelines",
        "sagemaker:listProcessingJobs",
        "sagemaker:listProjects",
        "sagemaker:listSpaces",
        "sagemaker:listStageDevices",
        "sagemaker:listStudioLifecycleConfigs",
        "sagemaker:listSubscribedWorkteams",
        "sagemaker:listTags",
        "sagemaker:listTrainingJobs",
        "sagemaker:listTrainingJobsForHyperParameterTuningJob",
        "sagemaker:listTransformJobs",
```

```
        "sagemaker:listTrialComponents",
        "sagemaker:listTrials",
        "sagemaker:listUserProfiles",
        "sagemaker:listWorkforces",
        "sagemaker:listWorkteams",
        "savingsplans:describeSavingsPlans",
        "scheduler:getSchedule",
        "scheduler:getScheduleGroup",
        "scheduler:listScheduleGroups",
        "scheduler:listSchedules",
        "schemas:describeCodeBinding",
        "schemas:describeDiscoverer",
        "schemas:describeRegistry",
        "schemas:describeSchema",
        "schemas:getCodeBindingSource",
        "schemas:getDiscoveredSchema",
        "schemas:getResourcePolicy",
        "schemas:listDiscoverers",
        "schemas:listRegistries",
        "schemas:listSchemas",
        "schemas:listSchemaVersions",
        "sdb:domainMetadata",
        "sdb:listDomains",
        "secretsmanager:describeSecret",
        "secretsmanager:getResourcePolicy",
        "secretsmanager:listSecrets",
        "secretsmanager:listSecretVersionIds",
        "securityhub:batchGetAutomationRules",
        "securityhub:batchGetConfigurationPolicyAssociations",
        "securityhub:describeOrganizationConfiguration",
        "securityhub:getConfigurationPolicy",
        "securityhub:getConfigurationPolicyAssociation",
        "securityhub:getEnabledStandards",
        "securityhub:getFindingAggregator",
        "securityhub:getFindingHistory",
        "securityhub:getFindings",
        "securityhub:getInsightResults",
        "securityhub:getInsights",
        "securityhub:getMasterAccount",
        "securityhub:getMembers",
        "securityhub:listAutomationRules",
        "securityhub:listConfigurationPolicies",
        "securityhub:listConfigurationPolicyAssociations",
        "securityhub:listEnabledProductsForImport",
```

```
        "securityhub:listFindingAggregators",
        "securityhub:listInvitations",
        "securityhub:listMembers",
        "securitylake:getDataLakeExceptionSubscription",
        "securitylake:getDataLakeOrganizationConfiguration",
        "securitylake:getDataLakeSources",
        "securitylake:getSubscriber",
        "securitylake:listDataLakeExceptions",
        "securitylake:listDataLakes",
        "securitylake:listLogSources",
        "securitylake:listSubscribers",
        "serverlessrepo:getApplication",
        "serverlessrepo:getApplicationPolicy",
        "serverlessrepo:getCloudFormationTemplate",
        "serverlessrepo:listApplicationDependencies",
        "serverlessrepo:listApplications",
        "serverlessrepo:listApplicationVersions",
        "servicecatalog:describeConstraint",
        "servicecatalog:describePortfolio",
        "servicecatalog:describeProduct",
        "servicecatalog:describeProductAsAdmin",
        "servicecatalog:describeProductView",
        "servicecatalog:describeProvisioningArtifact",
        "servicecatalog:describeProvisioningParameters",
        "servicecatalog:describeRecord",
        "servicecatalog:listAcceptedPortfolioShares",
        "servicecatalog:listConstraintsForPortfolio",
        "servicecatalog:listLaunchPaths",
        "servicecatalog:listPortfolioAccess",
        "servicecatalog:listPortfolios",
        "servicecatalog:listPortfoliosForProduct",
        "servicecatalog:listPrincipalsForPortfolio",
        "servicecatalog:listProvisioningArtifacts",
        "servicecatalog:listRecordHistory",
        "servicecatalog:scanProvisionedProducts",
        "servicecatalog:searchProducts",
        "servicequotas:getAssociationForServiceQuotaTemplate",
        "servicequotas:getAWSDefaultServiceQuota",
        "servicequotas:getRequestedServiceQuotaChange",
        "servicequotas:getServiceQuota",
        "servicequotas:getServiceQuotaIncreaseRequestFromTemplate",
        "servicequotas:listAWSDefaultServiceQuotas",
        "servicequotas:listRequestedServiceQuotaChangeHistory",
        "servicequotas:listRequestedServiceQuotaChangeHistoryByQuota",
```

```
        "servicequotas:listServiceQuotaIncreaseRequestsInTemplate",
        "servicequotas:listServiceQuotas",
        "servicequotas:listServices",
        "ses:batchGetMetricData",
        "ses:describeActiveReceiptRuleSet",
        "ses:describeConfigurationSet",
        "ses:describeReceiptRule",
        "ses:describeReceiptRuleSet",
        "ses:getAccount",
        "ses:getAccountSendingEnabled",
        "ses:getAddonInstance",
        "ses:getAddonSubscription",
        "ses:getArchive",
        "ses:getArchiveExport",
        "ses:getArchiveSearch",
        "ses:getBlacklistReports",
        "ses:getConfigurationSet",
        "ses:getConfigurationSetEventDestinations",
        "ses:getContactList",
        "ses:getDedicatedIp",
        "ses:getDedicatedIpPool",
        "ses:getDedicatedIps",
        "ses:getDeliverabilityDashboardOptions",
        "ses:getDeliverabilityTestReport",
        "ses:getDomainDeliverabilityCampaign",
        "ses:getDomainStatisticsReport",
        "ses:getEmailIdentity",
        "ses:getIdentityDkimAttributes",
        "ses:getIdentityMailFromDomainAttributes",
        "ses:getIdentityNotificationAttributes",
        "ses:getIdentityPolicies",
        "ses:getIdentityVerificationAttributes",
        "ses:getImportJob",
        "ses:getIngressPoint",
        "ses:getMessageInsights",
        "ses:getRelay",
        "ses:getRuleSet",
        "ses:getTrafficPolicy",
        "ses:getSendQuota",
        "ses:getSendStatistics",
        "ses:listConfigurationSets",
        "ses:listAddonInstances",
        "ses:listAddonSubscriptions",
        "ses:listArchiveExports",
```

```
        "ses:listArchives",
        "ses:listArchiveSearches",
        "ses:listContactLists",
        "ses:listContacts",
        "ses:listCustomVerificationEmailTemplates",
        "ses:listDedicatedIpPools",
        "ses:listDeliverabilityTestReports",
        "ses:listDomainDeliverabilityCampaigns",
        "ses:listEmailIdentities",
        "ses:listEmailTemplates",
        "ses:listIdentities",
        "ses:listIdentityPolicies",
        "ses:listImportJobs",
        "ses:listIngressPoints",
        "ses:listReceiptFilters",
        "ses:listReceiptRuleSets",
        "ses:listRelays",
        "ses:listRuleSets",
        "ses:listRecommendations",
        "ses:listTagsForResource",
        "ses:listTemplates",
        "ses:listTrafficPolicies",
        "ses:listVerifiedEmailAddresses",
        "shield:describeAttack",
        "shield:describeProtection",
        "shield:describeSubscription",
        "shield:listAttacks",
        "shield:listProtections",
        "signer:describeSigningJob",
        "signer:getRevocationStatus",
        "signer:getSigningPlatform",
        "signer:getSigningProfile",
        "signer:listProfilePermissions",
        "signer:listSigningJobs",
        "signer:listSigningPlatforms",
        "signer:listSigningProfiles",
        "sms-voice:getConfigurationSetEventDestinations",
        "sms:getConnectors",
        "sms:getReplicationJobs",
        "sms:getReplicationRuns",
        "sms:getServers",
        "snowball:describeAddress",
        "snowball:describeAddresses",
        "snowball:describeJob",
```

```
        "snowball:getSnowballUsage",
        "snowball:listJobs",
        "snowball:listServiceVersions",
        "sns:checkIfPhoneNumberIsOptedOut",
        "sns:getDataProtectionPolicy",
        "sns:getEndpointAttributes",
        "sns:getPlatformApplicationAttributes",
        "sns:getSMSAttributes",
        "sns:getSMSSandboxAccountStatus",
        "sns:getSubscriptionAttributes",
        "sns:getTopicAttributes",
        "sns:listEndpointsByPlatformApplication",
        "sns:listOriginationNumbers",
        "sns:listPhoneNumbersOptedOut",
        "sns:listPlatformApplications",
        "sns:listSMSSandboxPhoneNumbers",
        "sns:listSubscriptions",
        "sns:listSubscriptionsByTopic",
        "sns:listTopics",
        "sqs:getQueueAttributes",
        "sqs:getQueueUrl",
        "sqs:listDeadLetterSourceQueues",
        "sqs:listMessageMoveTasks",
        "sqs:listQueues",
        "ssm-contacts:describeEngagement",
        "ssm-contacts:describePage",
        "ssm-contacts:getContact",
        "ssm-contacts:getContactChannel",
        "ssm-contacts:getContactPolicy",
        "ssm-contacts:getRotation",
        "ssm-contacts:getRotationOverride",
        "ssm-contacts:listContactChannels",
        "ssm-contacts:listContacts",
        "ssm-contacts:listEngagements",
        "ssm-contacts:listPageReceipts",
        "ssm-contacts:listPageResolutions",
        "ssm-contacts:listPagesByContact",
        "ssm-contacts:listPagesByEngagement",
        "ssm-contacts:listPreviewRotationShifts",
        "ssm-contacts:listRotationOverrides",
        "ssm-contacts:listRotations",
        "ssm-contacts:listRotationShifts",
        "ssm-incidents:batchGetIncidentFindings",
        "ssm-incidents:getIncidentRecord",
```

```
        "ssm-incidents:getReplicationSet",
        "ssm-incidents:getResourcePolicies",
        "ssm-incidents:getResponsePlan",
        "ssm-incidents:getTimelineEvent",
        "ssm-incidents:listIncidentFindings",
        "ssm-incidents:listIncidentRecords",
        "ssm-incidents:listRelatedItems",
        "ssm-incidents:listReplicationSets",
        "ssm-incidents:listResponsePlans",
        "ssm-incidents:listTimelineEvents",
        "ssm-quicksetup:getConfiguration",
        "ssm-quicksetup:getConfigurationManager",
        "ssm-quicksetup:getServiceSettings",
        "ssm-quicksetup:listConfigurationManagers",
        "ssm-quicksetup:listConfigurations",
        "ssm-quicksetup:listQuickSetupTypes",
        "ssm-sap:getApplication",
        "ssm-sap:getComponent",
        "ssm-sap:getDatabase",
        "ssm-sap:getOperation",
        "ssm-sap:getResourcePermission",
        "ssm-sap:listApplications",
        "ssm-sap:listComponents",
        "ssm-sap:listDatabases",
        "ssm-sap:listOperations",
        "ssm:describeActivations",
        "ssm:describeAssociation",
        "ssm:describeAssociationExecutions",
        "ssm:describeAssociationExecutionTargets",
        "ssm:describeAutomationExecutions",
        "ssm:describeAutomationStepExecutions",
        "ssm:describeAvailablePatches",
        "ssm:describeDocument",
        "ssm:describeDocumentPermission",
        "ssm:describeEffectiveInstanceAssociations",
        "ssm:describeEffectivePatchesForPatchBaseline",
        "ssm:describeInstanceAssociationsStatus",
        "ssm:describeInstanceInformation",
        "ssm:describeInstancePatches",
        "ssm:describeInstancePatchStates",
        "ssm:describeInstancePatchStatesForPatchGroup",
        "ssm:describeInstanceProperties",
        "ssm:describeInventoryDeletions",
        "ssm:describeMaintenanceWindowExecutions",
```

```
        "ssm:describeMaintenanceWindowExecutionTaskInvocations",
        "ssm:describeMaintenanceWindowExecutionTasks",
        "ssm:describeMaintenanceWindows",
        "ssm:describeMaintenanceWindowSchedule",
        "ssm:describeMaintenanceWindowsForTarget",
        "ssm:describeMaintenanceWindowTargets",
        "ssm:describeMaintenanceWindowTasks",
        "ssm:describeOpsItems",
        "ssm:describeParameters",
        "ssm:describePatchBaselines",
        "ssm:describePatchGroups",
        "ssm:describePatchGroupState",
        "ssm:describePatchProperties",
        "ssm:describeSessions",
        "ssm:getAutomationExecution",
        "ssm:getCalendarState",
        "ssm:getCommandInvocation",
        "ssm:getConnectionStatus",
        "ssm:getDefaultPatchBaseline",
        "ssm:getDeployablePatchSnapshotForInstance",
        "ssm:getInventorySchema",
        "ssm:getMaintenanceWindow",
        "ssm:getMaintenanceWindowExecution",
        "ssm:getMaintenanceWindowExecutionTask",
        "ssm:getMaintenanceWindowExecutionTaskInvocation",
        "ssm:getMaintenanceWindowTask",
        "ssm:getOpsItem",
        "ssm:getOpsMetadata",
        "ssm:getOpsSummary",
        "ssm:getPatchBaseline",
        "ssm:getPatchBaselineForPatchGroup",
        "ssm:getResourcePolicies",
        "ssm:getServiceSetting",
        "ssm:listAssociations",
        "ssm:listAssociationVersions",
        "ssm:listCommandInvocations",
        "ssm:listCommands",
        "ssm:listComplianceItems",
        "ssm:listComplianceSummaries",
        "ssm:listDocumentMetadataHistory",
        "ssm:listDocuments",
        "ssm:listDocumentVersions",
        "ssm:listNodes",
        "ssm:listNodesSummary",
```

```
        "ssm:listOpsItemEvents",
        "ssm:listOpsItemRelatedItems",
        "ssm:listOpsMetadata",
        "ssm:listResourceComplianceSummaries",
        "ssm:listResourceDataSync",
        "ssm:listTagsForResource",
        "sso:describeApplication",
        "sso:describeApplicationAssignment",
        "sso:describeApplicationProvider",
        "sso:describeAccountAssignmentCreationStatus",
        "sso:describeAccountAssignmentDeletionStatus",
        "sso:describeInstance",
        "sso:describeInstanceAccessControlAttributeConfiguration",
        "sso:describePermissionSet",
        "sso:describePermissionSetProvisioningStatus",
        "sso:describeTrustedTokenIssuer",
        "sso:getApplicationAccessScope",
        "sso:getApplicationAssignmentConfiguration",
        "sso:getApplicationAuthenticationMethod",
        "sso:getApplicationGrant",
        "sso:getApplicationInstance",
        "sso:getApplicationTemplate",
        "sso:getInlinePolicyForPermissionSet",
        "sso:getManagedApplicationInstance",
        "sso:getPermissionsBoundaryForPermissionSet",
        "sso:getSharedSsoConfiguration",
        "sso:listApplicationAccessScopes",
        "sso:listApplicationAssignments",
        "sso:listApplicationAuthenticationMethods",
        "sso:listApplicationGrants",
        "sso:listApplicationInstances",
        "sso:listApplicationProviders",
        "sso:listApplications",
        "sso:listApplicationTemplates",
        "sso:listAccountAssignmentCreationStatus",
        "sso:listAccountAssignmentDeletionStatus",
        "sso:listAccountAssignments",
        "sso:listAccountAssignmentsForPrincipal",
        "sso:listAccountsForProvisionedPermissionSet",
        "sso:listApplicationAssignmentsForPrincipal",
        "sso:listCustomerManagedPolicyReferencesInPermissionSet",
        "sso:listDirectoryAssociations",
        "sso:listInstances",
        "sso:listManagedPoliciesInPermissionSet",
```

```
        "sso:listPermissionSetProvisioningStatus",
        "sso:listPermissionSets",
        "sso:listPermissionSetsProvisionedToAccount",
        "sso:listProfileAssociations",
        "sso:listTrustedTokenIssuers",
        "states:describeActivity",
        "states:describeExecution",
        "states:describeMapRun",
        "states:describeStateMachine",
        "states:describeStateMachineAlias",
        "states:describeStateMachineForExecution",
        "states:getExecutionHistory",
        "states:listActivities",
        "states:listExecutions",
        "states:listMapRuns",
        "states:listStateMachineAliases",
        "states:listStateMachines",
        "states:listStateMachineVersions",
        "storagegateway:describeBandwidthRateLimit",
        "storagegateway:describeCache",
        "storagegateway:describeCachediSCSIVolumes",
        "storagegateway:describeFileSystemAssociations",
        "storagegateway:describeGatewayInformation",
        "storagegateway:describeMaintenanceStartTime",
        "storagegateway:describeNFSFileShares",
        "storagegateway:describeSMBFileShares",
        "storagegateway:describeSMBSettings",
        "storagegateway:describeSnapshotSchedule",
        "storagegateway:describeStorediSCSIVolumes",
        "storagegateway:describeTapeArchives",
        "storagegateway:describeTapeRecoveryPoints",
        "storagegateway:describeTapes",
        "storagegateway:describeUploadBuffer",
        "storagegateway:describeVTLDevices",
        "storagegateway:describeWorkingStorage",
        "storagegateway:listAutomaticTapeCreationPolicies",
        "storagegateway:listFileShares",
        "storagegateway:listFileSystemAssociations",
        "storagegateway:listGateways",
        "storagegateway:listLocalDisks",
        "storagegateway:listTagsForResource",
        "storagegateway:listTapes",
        "storagegateway:listVolumeInitiators",
        "storagegateway:listVolumeRecoveryPoints",
```

```
        "storagegateway:listVolumes",
        "sts:getCallerIdentity",
        "swf:countClosedWorkflowExecutions",
        "swf:countOpenWorkflowExecutions",
        "swf:countPendingActivityTasks",
        "swf:countPendingDecisionTasks",
        "swf:describeActivityType",
        "swf:describeDomain",
        "swf:describeWorkflowExecution",
        "swf:describeWorkflowType",
        "swf:getWorkflowExecutionHistory",
        "swf:listActivityTypes",
        "swf:listClosedWorkflowExecutions",
        "swf:listDomains",
        "swf:listOpenWorkflowExecutions",
        "swf:listWorkflowTypes",
        "synthetics:describeCanaries",
        "synthetics:describeCanariesLastRun",
        "synthetics:describeRuntimeVersions",
        "synthetics:getCanary",
        "synthetics:getCanaryRuns",
        "synthetics:getGroup",
        "synthetics:listAssociatedGroups",
        "synthetics:listGroupResources",
        "synthetics:listGroups",
        "thinclient:getDevice",
        "thinclient:getEnvironment",
        "thinclient:getSoftwareSet",
        "thinclient:listDevices",
        "thinclient:listEnvironments",
        "thinclient:listSoftwareSets",
        "timestream:describeAccountSettings",
        "timestream:describeBatchLoadTask",
        "timestream:describeDatabase",
        "timestream:describeEndpoints",
        "timestream:describeScheduledQuery",
        "timestream:describeTable",
        "timestream:listBatchLoadTasks",
        "timestream:listDatabases",
        "timestream:listScheduledQueries",
        "timestream:listTables",
        "tiros:createQuery",
        "tiros:getQueryAnswer",
        "tiros:getQueryExplanation",
```

```
        "tnb:getSolFunctionInstance",
        "tnb:getSolFunctionPackage",
        "tnb:getSolNetworkInstance",
        "tnb:getSolNetworkOperation",
        "tnb:getSolNetworkPackage",
        "tnb:listSolFunctionInstances",
        "tnb:listSolFunctionPackages",
        "tnb:listSolNetworkInstances",
        "tnb:listSolNetworkOperations",
        "tnb:listSolNetworkPackages",
        "transcribe:describeLanguageModel",
        "transcribe:getCallAnalyticsCategory",
        "transcribe:getCallAnalyticsJob",
        "transcribe:getMedicalTranscriptionJob",
        "transcribe:getMedicalVocabulary",
        "transcribe:getTranscriptionJob",
        "transcribe:getVocabulary",
        "transcribe:getVocabularyFilter",
        "transcribe:listCallAnalyticsCategories",
        "transcribe:listCallAnalyticsJobs",
        "transcribe:listLanguageModels",
        "transcribe:listMedicalTranscriptionJobs",
        "transcribe:listMedicalVocabularies",
        "transcribe:listTranscriptionJobs",
        "transcribe:listVocabularies",
        "transcribe:listVocabularyFilters",
        "transfer:describeAccess",
        "transfer:describeAgreement",
        "transfer:describeConnector",
        "transfer:describeExecution",
        "transfer:describeProfile",
        "transfer:describeServer",
        "transfer:describeUser",
        "transfer:describeWebApp",
        "transfer:describeWebAppCustomization",
        "transfer:describeWorkflow",
        "transfer:listAccesses",
        "transfer:listAgreements",
        "transfer:listConnectors",
        "transfer:listExecutions",
        "transfer:listHostKeys",
        "transfer:listProfiles",
        "transfer:listServers",
        "transfer:listTagsForResource",
```

```
        "transfer:listUsers",
        "transfer:listWebApps",
        "transfer:listWorkflows",
        "transfer:sendWorkflowStepState",
        "trustedadvisor:getOrganizationRecommendation",
        "trustedadvisor:getRecommendation",
        "trustedadvisor:listChecks",
        "trustedadvisor:listOrganizationRecommendationAccounts",
        "trustedadvisor:listOrganizationRecommendationResources",
        "trustedadvisor:listOrganizationRecommendations",
        "trustedadvisor:listRecommendationResources",
        "trustedadvisor:listRecommendations",
        "verifiedpermissions:getIdentitySource",
        "verifiedpermissions:getPolicy",
        "verifiedpermissions:getPolicyStore",
        "verifiedpermissions:getPolicyTemplate",
        "verifiedpermissions:getSchema",
        "verifiedpermissions:listIdentitySources",
        "verifiedpermissions:listPolicies",
        "verifiedpermissions:listPolicyStores",
        "verifiedpermissions:listPolicyTemplates",
        "vpc-lattice:getAccessLogSubscription",
        "vpc-lattice:getAuthPolicy",
        "vpc-lattice:getListener",
        "vpc-lattice:getResourceConfiguration",
        "vpc-lattice:getResourceGateway",
        "vpc-lattice:getResourcePolicy",
        "vpc-lattice:getRule",
        "vpc-lattice:getService",
        "vpc-lattice:getServiceNetwork",
        "vpc-lattice:getServiceNetworkResourceAssociation",
        "vpc-lattice:getServiceNetworkServiceAssociation",
        "vpc-lattice:getServiceNetworkVpcAssociation",
        "vpc-lattice:getTargetGroup",
        "vpc-lattice:listAccessLogSubscriptions",
        "vpc-lattice:listListeners",
        "vpc-lattice:listResourceConfigurations",
        "vpc-lattice:listResourceGateways",
        "vpc-lattice:listRules",
        "vpc-lattice:listServiceNetworks",
        "vpc-lattice:listServiceNetworkResourceAssociations",
        "vpc-lattice:listServiceNetworkServiceAssociations",
        "vpc-lattice:listServiceNetworkVpcAssociations",
        "vpc-lattice:listServices",
```

```
        "vpc-lattice:listTargetGroups",
        "vpc-lattice:listTargets",
        "waf-regional:getByteMatchSet",
        "waf-regional:getChangeTokenStatus",
        "waf-regional:getGeoMatchSet",
        "waf-regional:getIPSet",
        "waf-regional:getLoggingConfiguration",
        "waf-regional:getRateBasedRule",
        "waf-regional:getRegexMatchSet",
        "waf-regional:getRegexPatternSet",
        "waf-regional:getRule",
        "waf-regional:getRuleGroup",
        "waf-regional:getSqlInjectionMatchSet",
        "waf-regional:getWebACL",
        "waf-regional:getWebACLForResource",
        "waf-regional:listActivatedRulesInRuleGroup",
        "waf-regional:listByteMatchSets",
        "waf-regional:listGeoMatchSets",
        "waf-regional:listIPSets",
        "waf-regional:listLoggingConfigurations",
        "waf-regional:listRateBasedRules",
        "waf-regional:listRegexMatchSets",
        "waf-regional:listRegexPatternSets",
        "waf-regional:listResourcesForWebACL",
        "waf-regional:listRuleGroups",
        "waf-regional:listRules",
        "waf-regional:listSqlInjectionMatchSets",
        "waf-regional:listWebACLs",
        "waf:getByteMatchSet",
        "waf:getChangeTokenStatus",
        "waf:getGeoMatchSet",
        "waf:getIPSet",
        "waf:getLoggingConfiguration",
        "waf:getRateBasedRule",
        "waf:getRegexMatchSet",
        "waf:getRegexPatternSet",
        "waf:getRule",
        "waf:getRuleGroup",
        "waf:getSampledRequests",
        "waf:getSizeConstraintSet",
        "waf:getSqlInjectionMatchSet",
        "waf:getWebACL",
        "waf:getXssMatchSet",
        "waf:listActivatedRulesInRuleGroup",
```

```
        "waf:listByteMatchSets",
        "waf:listGeoMatchSets",
        "waf:listIPSets",
        "waf:listLoggingConfigurations",
        "waf:listRateBasedRules",
        "waf:listRegexMatchSets",
        "waf:listRegexPatternSets",
        "waf:listRuleGroups",
        "waf:listRules",
        "waf:listSizeConstraintSets",
        "waf:listSqlInjectionMatchSets",
        "waf:listWebACLs",
        "waf:listXssMatchSets",
        "wafv2:checkCapacity",
        "wafv2:describeManagedRuleGroup",
        "wafv2:getIPSet",
        "wafv2:getLoggingConfiguration",
        "wafv2:getPermissionPolicy",
        "wafv2:getRateBasedStatementManagedKeys",
        "wafv2:getRegexPatternSet",
        "wafv2:getRuleGroup",
        "wafv2:getSampledRequests",
        "wafv2:getWebACL",
        "wafv2:getWebACLForResource",
        "wafv2:listAvailableManagedRuleGroups",
        "wafv2:listIPSets",
        "wafv2:listLoggingConfigurations",
        "wafv2:listRegexPatternSets",
        "wafv2:listResourcesForWebACL",
        "wafv2:listRuleGroups",
        "wafv2:listTagsForResource",
        "wafv2:listWebACLs",
        "workdocs:checkAlias",
        "workdocs:describeAvailableDirectories",
        "workdocs:describeInstances",
        "workmail:describeGroup",
        "workmail:describeOrganization",
        "workmail:describeResource",
        "workmail:describeUser",
        "workmail:listAliases",
        "workmail:listGroupMembers",
        "workmail:listGroups",
        "workmail:listMailboxPermissions",
        "workmail:listOrganizations",
```

```
        "workmail:listResourceDelegates",
        "workmail:listResources",
        "workmail:listUsers",
        "workspaces-web:getBrowserSettings",
        "workspaces-web:getIdentityProvider",
        "workspaces-web:getNetworkSettings",
        "workspaces-web:getPortal",
        "workspaces-web:getPortalServiceProviderMetadata",
        "workspaces-web:getTrustStoreCertificate",
        "workspaces-web:getUserSettings",
        "workspaces-web:listBrowserSettings",
        "workspaces-web:listIdentityProviders",
        "workspaces-web:listNetworkSettings",
        "workspaces-web:listPortals",
        "workspaces-web:listTagsForResource",
        "workspaces-web:listTrustStoreCertificates",
        "workspaces-web:listTrustStores",
        "workspaces-web:listUserSettings",
        "workspaces:describeAccount",
        "workspaces:describeAccountModifications",
        "workspaces:describeApplicationAssociations",
        "workspaces:describeIpGroups",
        "workspaces:describeTags",
        "workspaces:describeWorkspaceAssociations",
        "workspaces:describeWorkspaceBundles",
        "workspaces:describeWorkspaceDirectories",
        "workspaces:describeWorkspaceImages",
        "workspaces:describeWorkspaces",
        "workspaces:describeWorkspaceSnapshots",
        "workspaces:describeWorkspacesConnectionStatus",
        "workspaces:describeWorkspacesPools",
        "workspaces:describeWorkspacesPoolSessions",
        "xray:getEncryptionConfig",
        "xray:getGroup",
        "xray:getGroups",
        "xray:getInsightImpactGraph",
        "xray:getSamplingRules",
        "xray:getSamplingStatisticSummaries",
        "xray:getSamplingTargets",
        "xray:getServiceGraph",
        "xray:getTimeSeriesServiceStatistics",
        "xray:getTraceGraph",
        "xray:listResourcePolicies"
      ],
```

```
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    }
  ],
  "Version" : "2012-10-17"
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSSystemsManagerAccountDiscoveryServicePolicy

説明: AWS AWS アカウント 情報を検出する Systems Manager (SSM) アクセス許可を付与します。

`AWSSystemsManagerAccountDiscoveryServicePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 10 月 24 日 17:21 UTC
- 編集日時: 2022 年 10 月 17 日 20:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerAccountDiscoveryServicePolicy`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSSystemsManagerChangeManagementServicePolicy

説明: AWS Systems Manager 変更管理フレームワークによって管理または使用される AWS リソースへのアクセスを提供します。

`AWSSystemsManagerChangeManagementServicePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 12 月 7 日 22:21 UTC
- 編集日時: 2025 年 10 月 23 日 21:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerChangeManagementServicePolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:DeleteAssociation",
        "ssm:CreateOpsItem",
        "ssm:GetOpsItem",
        "ssm:UpdateOpsItem",
        "ssm:StartAutomationExecution",
        "ssm:StopAutomationExecution",
        "ssm:GetAutomationExecution",
        "ssm:GetCalendarState",
        "ssm:GetDocument"
```

```
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sso:ListDirectoryAssociations"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:DescribeUsers",
        "sso-directory:IsMemberInGroup"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:GetGroup",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:*:sso:::instance/*"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityStore",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
 "arn:*:identitystore::*:identitystore/*"
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSSystemsManagerEnableConfigRecordingExecutionPolicy

説明: AWS Systems Manager Quick Setup が Config AWS 設定の記録を有効にして設定するためのアクセス許可を提供します。

AWSSystemsManagerEnableConfigRecordingExecutionPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSSystemsManagerEnableConfigRecordingExecutionPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 6 月 26 日 09:40 UTC
- 編集日時: 2024 年 6 月 26 日 09:40 UTC
- ARN: arn:aws:iam::aws:policy/AWSSystemsManagerEnableConfigRecordingExecutionPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Sid" : "S3BucketCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutBucketPublicAccessBlock",
        "s3:ListBucket",
        "s3:PutBucketPolicy",
        "s3:PutEncryptionConfiguration"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-quick-setup-config-recording-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SNSTopicsListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DefaultSNSTopicCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic"
      ],
      "Resource" : "arn:aws:sns:*:*:ConfigRecording-Default-Topic"
    },
    {
      "Sid" : "ConfigureAndStartConfigurationRecorderPermissions",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigurationRecorders",
        "config:DescribeDeliveryChannels",
        "config:PutConfigurationRecorder",
        "config:PutDeliveryChannel",
```

```
        "config:StartConfigurationRecorder"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetAndPassConfigSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/config.amazonaws.com/
AWSServiceRoleForConfig",
        "arn:aws:iam::*:role/AWSServiceRoleForConfig"
      ]
    },
    {
      "Sid" : "CreateConfigSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/config.amazonaws.com/
AWSServiceRoleForConfig"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "config.amazonaws.com"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSSystemsManagerEnableExplorerExecutionPolicy

説明: このポリシーは、 AWS Systems Manager の一機能である Explorer を有効にするための管理アクセス許可を付与します。これには、関連する Systems Manager サービス設定を更新し、Systems Manager のためにサービスリンクロールを作成する権限が含まれます。

`AWSSystemsManagerEnableExplorerExecutionPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSSystemsManagerEnableExplorerExecutionPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 6 月 26 日 09:42 UTC
- 編集日時: 2024 年 6 月 26 日 09:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerEnableExplorerExecutionPolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateSystemsManagerSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
```

```
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ReadOnlyPermissionsForEnablingExplorer",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "config:DescribeConfigurationRecorders",
        "compute-optimizer:GetEnrollmentStatus",
        "support:DescribeTrustedAdvisorChecks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMExplorerServiceSettingsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/ssm-patchmanager",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/EC2",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ExplorerOnboarded",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/Association",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ComputeOptimizer",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ConfigCompliance",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/OpsData-TrustedAdvisor",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/SupportCenterCase"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSSystemsManagerForSAPFullAccess

説明: AWS Systems Manager for SAP サービスへのフルアクセスを提供します

`AWSSystemsManagerForSAPFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSSystemsManagerForSAPFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 11 月 17 日 02:11 UTC
- 編集日時: 2024 年 7 月 10 日 21:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerForSAPFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Sid" : "AwsSsmForSapPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:*"
      ],
      "Resource" : "arn:*:ssm-sap:*:*:*"
    },
    {
      "Sid" : "AwsSsmForSapServiceRoleCreationPermission",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm-sap.amazonaws.com/
AWSServiceRoleForAWSSSMForSAP"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm-sap.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "Ec2StartStopPermission",
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "ec2:resourceTag/SSMForSAPManaged" : "True"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSSystemsManagerForSAPReadOnlyAccess

説明: AWS Systems Manager for SAP サービスへの読み取り専用アクセスを提供します

`AWSSystemsManagerForSAPReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSSystemsManagerForSAPReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 11 月 17 日 02:11 UTC
- 編集日時: 2022 年 11 月 17 日 02:11 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerForSAPReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:get*",
        "ssm-sap:list*"
      ],
      "Resource" : "arn:*:ssm-sap:*:*:*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSSystemsManagerJustInTimeAccessServicePolicy

説明: AWS Systems Manager がジャストインタイムアクセスフレームワークで管理または使用する AWS リソースへのアクセスを提供します。

`AWSSystemsManagerJustInTimeAccessServicePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2025 年 4 月 21 日 20:07 UTC
- 編集日時: 2025 年 10 月 23 日 21:19 UTC

- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerJustInTimeAccessServicePolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowOpsItemReplication",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateOpsItem"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:opsitem/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:RequestTag/SystemsManagerJustInTimeNodeAccessManaged" : "Replica"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SystemsManagerJustInTimeNodeAccessManaged"
          ]
        }
      }
    },
    {
      "Sid" : "AllowOpsItemReplicationTagging",
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource"
```

```
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:opsitem/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SystemsManagerJustInTimeNodeAccessManaged" : "Replica"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SystemsManagerJustInTimeNodeAccessManaged"
          ]
        }
      }
    },
    {
      "Sid" : "AllowAutomationExecutionTagging",
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-execution/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SystemsManagerJustInTimeNodeAccessManaged" : "true"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SystemsManagerJustInTimeNodeAccessManaged"
          ]
        }
      }
    },
    {
      "Sid" : "AllowOpsItemManagement",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetOpsItem",
        "ssm:UpdateOpsItem"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:opsitem/*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowRetrieveDocument",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetDocument",
        "ssm:DescribeDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ssm:DocumentType" : [
            "ManualApprovalPolicy",
            "AutoApprovalPolicy"
          ]
        }
      }
    },
    {
      "Sid" : "AllowDescriptions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeOpsItems",
        "ssm:DescribeSessions",
        "ssm:ListDocuments"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowListTagsForManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListTagsForResource"
      ],
```

```
      "Resource" : [
        "arn:aws:ssm:*:*:managed-instance/*"
      ]
    },
    {
      "Sid" : "AllowListSSMGUIConnections",
      "Effect" : "Allow",
      "Action" : [
        "ssm-guiconnect:ListConnections"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowIdentityStoreActions",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:ListGroupMembershipsForMember",
        "identitystore:DescribeUser",
        "identitystore:GetGroupId",
        "identitystore:GetUserId"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowSSODirectoryActions",
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:DescribeUsers",
        "sso-directory:IsMemberInGroup"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowSSOInstanceActions",
      "Effect" : "Allow",
      "Action" : [
        "sso:ListInstances",
        "sso:DescribeRegisteredRegions",
```

```
        "sso:ListDirectoryAssociations"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowDescribingEC2Tags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeTags"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowPublishingCloudWatchMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/SSM/JustInTimeAccess"
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:*:sso:::instance/*"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
```

```
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityStore",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
 "arn:*:identitystore::*:identitystore/*"
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSSystemsManagerJustInTimeAccessTokenPolicy

説明: マネージドポリシー AWSSystemsManagerJustInTimeAccessTokenPolicy により、Systems Manager はジャストインタイムノードアクセスに使用されるアクセストークンを生成できます。

AWSSystemsManagerJustInTimeAccessTokenPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSSystemsManagerJustInTimeAccessTokenPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 4 月 17 日 21:07 UTC
- 編集日時: 2025 年 9 月 25 日 20:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerJustInTimeAccessTokenPolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SsmStartSession",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*:*:document/SSM-SessionManagerRunShell"
      ]
    },
    {
      "Sid" : "TerminateAndResumeSessionAndOpenDataChannel",
      "Effect" : "Allow",
      "Action" : [
        "ssm:TerminateSession",
        "ssm:ResumeSession",
        "ssmmessages:OpenDataChannel"
      ],
```

```
      "Resource" : "arn:aws:ssm:*:*:session/*"
    },
    {
      "Sid" : "GuiConnect",
      "Effect" : "Allow",
      "Action" : [
        "ssm-guiconnect:CancelConnection",
        "ssm-guiconnect:GetConnection",
        "ssm-guiconnect:StartConnection"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SessionManagerKmsPermission",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SystemsManagerJustInTimeNodeAccessManaged" : "true"
        }
      }
    },
    {
      "Sid" : "RdpKmsPermission",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SystemsManagerJustInTimeNodeAccessManaged" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : "ssm-guiconnect.*.amazonaws.com"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
```

```
    {
      "Sid" : "RdpStartSession",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*:*:document/AWS-StartPortForwardingSession"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "ssm-guiconnect.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SsmRdpSsoSetup",
      "Effect" : "Allow",
      "Action" : [
        "sso:ListDirectoryAssociations*",
        "identitystore:DescribeUser",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "ssm-guiconnect.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SsmRdpSsoSetupSendCommand",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*:*:document/AWSSSO-CreateSSOUser"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:CalledViaFirst" : "ssm-guiconnect.amazonaws.com"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSSystemsManagerJustInTimeAccessTokenSessionPolicy

説明: マネージドポリシー AWSSystemsManagerJustInTimeAccessTokenSessionPolicy により、Systems Manager はスコープダウンされたアクセス許可を起動後のジャストインタイムノードアクセスセッションに適用できます。

`AWSSystemsManagerJustInTimeAccessTokenSessionPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSSystemsManagerJustInTimeAccessTokenSessionPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 4 月 17 日 20:52 UTC
- 編集日時: 2025 年 4 月 17 日 20:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerJustInTimeAccessTokenSessionPolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SsmStartSession",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/SSM-SessionManagerRunShell"
      ]
    },
    {
      "Sid" : "GuiConnect",
      "Effect" : "Allow",
      "Action" : [
        "ssm-guiconnect:CancelConnection",
        "ssm-guiconnect:GetConnection",
        "ssm-guiconnect:StartConnection"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SessionManagerKmsPermission",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SystemsManagerJustInTimeNodeAccessManaged" : "true"
```

```
        }
      }
    },
    {
      "Sid" : "RdpKmsPermission",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SystemsManagerJustInTimeNodeAccessManaged" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : "ssm-guiconnect.*.amazonaws.com"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "RdpStartSession",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-StartPortForwardingSession"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "ssm-guiconnect.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SsmRdpSsoSetup",
      "Effect" : "Allow",
      "Action" : [
        "sso:ListDirectoryAssociations*",
        "identitystore:DescribeUser",
        "ssm:GetCommandInvocation"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "ssm-guiconnect.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SsmRdpSsoSetupSendCommand",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSSSO-CreateSSOUser"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "ssm-guiconnect.amazonaws.com"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy

説明: このポリシーにより、Systems Manager は委任管理者アカウントからメンバーアカウントへのジャストインタイムノードアクセスの拒否アクセスポリシーを共有し、ポリシーを複数のリージョンにレプリケートできます。

AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 4 月 21 日 20:52 UTC
- 編集日時: 2025 年 4 月 23 日 21:07 UTC
- ARN: arn:aws:iam::aws:policy/AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "QuickSetupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-quicksetup:ListConfigurationManagers",
        "ssm-quicksetup:GetConfigurationManager",
        "cloudformation:ListStackSets"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "QuickSetupOrganizationsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "ssm-quicksetup.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "QuickSetupSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm-quicksetup.amazonaws.com/
AWSServiceRoleForSSMQuickSetup"
      ]
    },
    {
      "Sid" : "OrganizationsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMDocumentPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetDocument",
        "ssm:DescribeDocument",
        "ssm:ListTagsForResource",
        "ssm:PutResourcePolicy",
        "ssm:DeleteResourcePolicy",
        "ssm:GetResourcePolicies"
      ],
```

```
      "Resource" : "arn:aws:ssm:*:*:document/SSM-JustInTimeAccessDenyAccessOrgPolicy",
      "Condition" : {
        "StringEquals" : {
          "ssm:DocumentType" : "AutoApprovalPolicy"
        }
      }
    },
    {
      "Sid" : "SSMDocumentCreateReplicaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateDocument"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/SSM-JustInTimeAccessDenyAccessOrgPolicy",
      "Condition" : {
        "StringEquals" : {
          "ssm:DocumentType" : "AutoApprovalPolicy",
          "aws:RequestTag/SystemsManagerJustInTimeNodeAccessManaged" : "true"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SystemsManagerJustInTimeNodeAccessManaged"
          ]
        }
      }
    },
    {
      "Sid" : "SSMDocumentUpdateReplicaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateDocument",
        "ssm:UpdateDocumentDefaultVersion",
        "ssm:UpdateDocumentMetadata",
        "ssm:DeleteDocument",
        "ssm:AddTagsToResource",
        "ssm:RemoveTagsFromResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/SSM-JustInTimeAccessDenyAccessOrgPolicy",
      "Condition" : {
        "StringEquals" : {
          "ssm:DocumentType" : "AutoApprovalPolicy",
          "aws:ResourceTag/SystemsManagerJustInTimeNodeAccessManaged" : "true"
        }
      }
```

```
    },
    {
      "Sid" : "RAMReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShares",
        "ram:GetResourceShareAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RAMCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SystemsManagerJustInTimeNodeAccessManaged" : "true"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SystemsManagerJustInTimeNodeAccessManaged"
          ]
        },
        "StringEqualsIfExists" : {
          "ram:RequestedResourceType" : "ssm:Document"
        },
        "ArnLikeIfExists" : {
          "ram:ResourceArn" : "arn:aws:ssm:*:*:document/SSM-
JustInTimeAccessDenyAccessOrgPolicy"
        }
      }
    },
    {
      "Sid" : "RAMTaggingPermissions",
      "Effect" : "Allow",
      "Action" : "ram:TagResource",
      "Resource" : "arn:aws:ram:*:*:resource-share/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SystemsManagerJustInTimeNodeAccessManaged" : "true"
        },
```

```
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SystemsManagerJustInTimeNodeAccessManaged"
          ]
        }
      }
    },
    {
      "Sid" : "RAMModificationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ram:ResourceShareName" : "SSMJustInTimeNodeAccessManagedResourceShare",
          "aws:ResourceTag/SystemsManagerJustInTimeNodeAccessManaged" : "true"
        },
        "StringEqualsIfExists" : {
          "ram:RequestedResourceType" : "ssm:Document"
        },
        "ArnLikeIfExists" : {
          "ram:ResourceArn" : "arn:aws:ssm:*:*:document/SSM-
JustInTimeAccessDenyAccessOrgPolicy"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSSystemsManagerNotificationsServicePolicy

説明: ジャストインタイムノードアクセス通知のためにユーザーに関する情報を収集するために必要なアクセス許可。

AWSSystemsManagerNotificationsServicePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2025 年 4 月 17 日 20:52 UTC
- 編集日時: 2025 年 4 月 17 日 20:52 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerNotificationsServicePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowIdentityStoreActions",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:ListGroupMembershipsForMember",
```

```
        "identitystore:ListGroupMemberships",
        "identitystore:DescribeUser"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowSSOActions",
      "Effect" : "Allow",
      "Action" : [
        "sso:ListInstances",
        "sso:DescribeRegisteredRegions",
        "sso:ListDirectoryAssociations"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowSSODirectoryActions",
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:DescribeUser",
        "sso-directory:ListMembersInGroup"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowIamActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSSystemsManagerOpsDataSyncServiceRolePolicy

説明: OpsData 関連オペレーションを管理する SSM Explorer 向け IAM ロール

`AWSSystemsManagerOpsDataSyncServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 4 月 26 日 20:42 UTC
- 編集日時: 2023 年 6 月 28 日 22:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerOpsDataSyncServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSThinkboxAssetServerPolicy

説明: このポリシーは、 AWS ポータルアセットサーバーに通常のオペレーションに必要なアクセス許可を付与します。

AWSThinkboxAssetServerPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSThinkboxAssetServerPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 5 月 27 日 19:18 UTC

- 編集日時: 2020 年 5 月 27 日 19:18 UTC
- ARN: arn:aws:iam::aws:policy/AWSThinkboxAssetServerPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSThinkboxAWSPortalAdminPolicy

説明: このポリシーは、 AWS Thinkbox の Deadline ソフトウェアに、 AWS ポータル管理に必要な複数の AWS サービスへのフルアクセスを付与します。これには、複数の EC2 リソースタイプに任意のタグを作成するためのアクセス権限が含まれます。

AWSThinkboxAWSPortalAdminPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSThinkboxAWSPortalAdminPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 5 月 27 日 19:41 UTC
- 編集日時: 2024 年 11 月 12 日 19:22 UTC
- ARN: arn:aws:iam::aws:policy/AWSThinkboxAWSPortalAdminPolicy

ポリシーのバージョン

ポリシーのバージョン: v9 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSThinkboxAWSPortal1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachInternetGateway",
        "ec2:AssociateAddress",
        "ec2:AssociateRouteTable",
        "ec2:AllocateAddress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateFleet",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateInternetGateway",
        "ec2:CreateNatGateway",
        "ec2:CreatePlacementGroup",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateVpc",
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeAddresses",
        "ec2:DescribeFleets",
        "ec2:DescribeFleetHistory",
        "ec2:DescribeFleetInstances",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeRouteTables",
        "ec2:DescribeNatGateways",
        "ec2:DescribeTags",
        "ec2:DescribeKeyPairs",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeRegions",
        "ec2:DescribeSpotFleetRequestHistory",
        "ec2:DescribeSecurityGroups",
```

```
        "ec2:DescribeSpotFleetInstances",
        "ec2:DescribeSpotFleetRequests",
        "ec2:DescribeSpotPriceHistory",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:GetConsoleOutput",
        "ec2:ImportKeyPair",
        "ec2:ReleaseAddress",
        "ec2:RequestSpotFleet",
        "ec2:CancelSpotFleetRequests",
        "ec2:DisassociateAddress",
        "ec2:DeleteFleets",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteVpc",
        "ec2:DeletePlacementGroup",
        "ec2:DeleteVpcEndpoints",
        "ec2:DeleteInternetGateway",
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
        "ec2:DisassociateRouteTable",
        "ec2:DeleteSubnet",
        "ec2:DeleteNatGateway",
        "ec2:DetachInternetGateway",
        "ec2:ModifyInstanceAttribute",
        "ec2:ModifyFleet",
        "ec2:ModifySpotFleetRequest",
        "ec2:ModifyVpcAttribute"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSThinkboxAWSPortal2",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:security-group/*",
```

```
        "arn:aws:ec2:*:*:placement-group/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*::image/*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal3",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "ArnLike" : {
          "ec2:InstanceProfile" : "arn:aws:iam::*:instance-profile/AWSPortal*"
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal4",
      "Effect" : "Allow",
      "Action" : "ec2:TerminateInstances",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/aws:cloudformation:logical-id" : "ReverseForwarder"
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal5",
      "Effect" : "Allow",
      "Action" : "ec2:TerminateInstances",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/aws:ec2spot:fleet-request-id" : false
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal6",
      "Effect" : "Allow",
      "Action" : "ec2:TerminateInstances",
      "Resource" : "*",
      "Condition" : {
```

```
        "ArnLike" : {
          "ec2:PlacementGroup" : "arn:aws:ec2:*:*:placement-group/
*DeadlinePlacementGroup*"
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal7",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "ArnLike" : {
          "ec2:PlacementGroup" : "arn:aws:ec2:*:*:placement-group/
*DeadlinePlacementGroup*"
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal8",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:CreateAction" : "RunInstances"
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal9",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:internet-gateway/*",
```

```
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:natgateway/*",
        "arn:aws:ec2:*:*:elastic-ip/*"
      ]
    },
    {
      "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*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSThinkboxAWSPortalGatewayPolicy

説明: このポリシーは、通常のオペレーションに必要なアクセス許可を AWS Portal Gateway マシンに付与します。

AWSThinkboxAWSPortalGatewayPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSThinkboxAWSPortalGatewayPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 5 月 27 日 19:05 UTC
- 編集日時: 2020 年 6 月 30 日 16:02 UTC
- ARN: arn:aws:iam::aws:policy/AWSThinkboxAWSPortalGatewayPolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSThinkboxAWSPortalWorkerPolicy

説明: このポリシーは、 AWS ポータルの Deadline Workers に、通常のオペレーションに必要なアクセス許可を付与します。

`AWSThinkboxAWSPortalWorkerPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSThinkboxAWSPortalWorkerPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2020 年 5 月 27 日 19:15 UTC
- 編集日時: 2020 年 12 月 7 日 23:27 UTC
- ARN: arn:aws:iam::aws:policy/AWSThinkboxAWSPortalWorkerPolicy

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSThinkboxDeadlineResourceTrackerAccessPolicy

説明: AWS Thinkbox の Deadline Resource Tracker のオペレーションに必要なアクセス許可を付与します。これには、DeleteFleets や CancelSpotFleetRequests など、一部の EC2 アクションへのフルアクセスが含まれます。

`AWSThinkboxDeadlineResourceTrackerAccessPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSThinkboxDeadlineResourceTrackerAccessPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 5 月 27 日 19:25 UTC
- 編集日時: 2020 年 5 月 27 日 19:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxDeadlineResourceTrackerAccessPolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSThinkboxDeadlineResourceTrackerAdminPolicy

説明: AWS Thinkbox の Deadline Resource Tracker を作成、破棄、管理するために必要なアクセス許可を付与します。

AWSThinkboxDeadlineResourceTrackerAdminPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSThinkboxDeadlineResourceTrackerAdminPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 5 月 27 日 19:29 UTC
- 編集日時: 2024 年 11 月 12 日 19:29 UTC
- ARN: arn:aws:iam::aws:policy/AWSThinkboxDeadlineResourceTrackerAdminPolicy

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker1",
      "Effect" : "Allow",
      "Action" : [
```

```
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker2",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStacks"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker3",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:UpdateStack",
        "cloudformation:DescribeStacks",
        "cloudformation:UpdateTerminationProtection",
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DeadlineResourceTracker*"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker4",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:CreateTable",
        "dynamodb:DeleteTable",
        "dynamodb:DescribeTable",
```

```
        "dynamodb:ListTagsOfResource",
        "dynamodb:TagResource",
        "dynamodb:UntagResource"
      ],
      "Resource" : [
        "arn:aws:dynamodb:*:*:table/DeadlineEC2ComputeNodeHealth*",
        "arn:aws:dynamodb:*:*:table/DeadlineEC2ComputeNodeInfo*",
        "arn:aws:dynamodb:*:*:table/DeadlineFleetHealth*"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker5",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:BatchWriteItem",
        "dynamodb:Scan"
      ],
      "Resource" : [
        "arn:aws:dynamodb:*:*:table/DeadlineFleetHealth*"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker6",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/DeadlineResourceTracker*"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker7",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/DeadlineResourceTracker*"
```

```
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker8",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetUser"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker9",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "dynamodb.application-autoscaling.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker10",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/DeadlineResourceTrackerAccess*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lambda.amazonaws.com"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker11",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/dynamodb.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_DynamoDBTable"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "application-autoscaling.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker12",
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetEventSourceMapping"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker13",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateEventSourceMapping",
        "lambda:DeleteEventSourceMapping"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ArnLike" : {
          "lambda:FunctionArn" : [
            "arn:aws:lambda:*:*:function:DeadlineResourceTracker*"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker14",
      "Effect" : "Allow",
      "Action" : [
        "lambda:AddPermission",
        "lambda:RemovePermission"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:DeadlineResourceTracker*"
      ],
      "Condition" : {
        "StringLike" : {
          "lambda:Principal" : "events.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker15",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:DeleteFunctionConcurrency",
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:ListTags",
        "lambda:PutFunctionConcurrency",
        "lambda:TagResource",
        "lambda:UntagResource",
        "lambda:UpdateFunctionCode",
        "lambda:UpdateFunctionConfiguration"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:DeadlineResourceTracker*"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker16",
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*/deadline_aws_resource_tracker-*.zip",
        "arn:aws:s3:::*/DeadlineAWSResourceTrackerTemplate-*.yaml"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker17",
      "Effect" : "Allow",
      "Action" : [
        "sqs:CreateQueue",
        "sqs:DeleteQueue",
        "sqs:GetQueueAttributes",
        "sqs:ListQueueTags",
        "sqs:TagQueue",
        "sqs:UntagQueue"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:DeadlineAWSComputeNodeState*",
        "arn:aws:sqs:*:*:DeadlineResourceTracker*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSThinkboxDeadlineSpotEventPluginAdminPolicy

説明: AWS Thinkbox の Deadline Spot Event Plugin に必要なアクセス許可を付与します。これには、スポットフリートをリクエスト、変更、キャンセルする許可の他に、制限付きの PassRole 許可が含まれます。

AWSThinkboxDeadlineSpotEventPluginAdminPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSThinkboxDeadlineSpotEventPluginAdminPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 5 月 27 日 19:38 UTC
- 編集日時: 2020 年 5 月 27 日 19:38 UTC
- ARN: arn:aws:iam::aws:policy/AWSThinkboxDeadlineSpotEventPluginAdminPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSThinkboxDeadlineSpotEventPluginWorkerPolicy

説明: AWS Thinkbox Deadline スポットイベントプラグインワーカーソフトウェアを実行する EC2 インスタンスに必要なアクセス許可を付与します。

`AWSThinkboxDeadlineSpotEventPluginWorkerPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSThinkboxDeadlineSpotEventPluginWorkerPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 5 月 27 日 19:35 UTC
- 編集日時: 2020 年 12 月 7 日 23:31 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxDeadlineSpotEventPluginWorkerPolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSTransferConsoleFullAccess

説明: 経由で AWS 転送へのフルアクセスを提供します AWS マネジメントコンソール

`AWSTransferConsoleFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSTransferConsoleFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 12 月 14 日 19:33 UTC
- 編集日時: 2020 年 12 月 14 日 19:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransferConsoleFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSTransferFullAccess

説明: AWS Transfer Service へのフルアクセスを提供します。

`AWSTransferFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSTransferFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 12 月 14 日 19:37 UTC
- 編集日時: 2020 年 12 月 14 日 19:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransferFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSTransferLoggingAccess

説明: AWS Transfer フルアクセスを許可してログストリームとグループを作成し、アカウントにログイベントを配置する

`AWSTransferLoggingAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSTransferLoggingAccess` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2019 年 1 月 14 日 15:32 UTC
- 編集日時: 2019 年 1 月 14 日 15:32 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSTransferLoggingAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSTransferReadOnlyAccess

説明: AWS Transfer サービスへの読み取り専用アクセスを提供します。

`AWSTransferReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSTransferReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 8 月 27 日 17:54 UTC
- 編集日時: 2020 年 8 月 27 日 17:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransferReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "transfer:DescribeUser",
        "transfer:DescribeServer",
        "transfer:ListUsers",
        "transfer:ListServers",
        "transfer:TestIdentityProvider",
        "transfer:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSTransformApplicationDeploymentPolicy

説明: AWS 変換サービスが、 AWS リソースを作成および管理することで、変換された .NET アプリケーションをデプロイできるようにします。このポリシーは、インフラストラクチャのプロビジョニ

ング、コンピューティングリソースの管理、さまざまな AWS サービスにわたるデプロイ設定の構成を行うアクセス許可を付与します。

AWSTransformApplicationDeploymentPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSTransformApplicationDeploymentPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2025 年 8 月 28 日 06:34 UTC
- 編集日時: 2025 年 11 月 21 日 23:34 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSTransformApplicationDeploymentPolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      },
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/AWSTransform*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSTransform",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : "arn:aws:cloudformation:*:*:stack/AWSTransform*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DeleteStack"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSTransform",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : "arn:aws:cloudformation:*:*:stack/AWSTransform*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:UpdateStack"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSTransform",
          "aws:ResourceTag/CreatedBy" : "AWSTransform",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
```

```
      "Resource" : "arn:aws:cloudformation:*:*:stack/AWSTransform*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeRouteTables",
        "ec2:DescribeInternetGateways"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "ForAnyValue:StringNotEquals" : {
          "aws:TagKeys" : [
            "Name",
            "CreatedBy",
            "ApplicationName",
            "TransformationType",
            "aws:cloudformation:stack-name",
            "aws:cloudformation:logical-id",
            "aws:cloudformation:stack-id"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
```

```
          "aws:CalledVia" : "cloudformation.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cloudformation.amazonaws.com"
        }
      },
      "Resource" : [
        "arn:aws:ec2:*::image/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cloudformation.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetInstanceProfile",
        "iam:GetRolePolicy",
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWSTransform-Deploy-Builder-Instance-Role",
        "arn:aws:iam::*:instance-profile/AWSTransform-Deploy-Builder-Instance-Role",
        "arn:aws:iam::*:role/AWSTransform-Deploy-App-Instance-Role",
        "arn:aws:iam::*:instance-profile/AWSTransform-Deploy-App-Instance-Role"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWSTransform-Deploy-Builder-Instance-Role",
        "arn:aws:iam::*:role/AWSTransform-Deploy-App-Instance-Role"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameters"
      ],
      "Resource" : "arn:aws:ssm:*::parameter/aws/service/ami-amazon-linux-latest*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances",
        "ec2:StopInstances",
        "ec2:StartInstances",
        "ec2:ModifyInstanceAttribute"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSTransform",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cloudformation.amazonaws.com"
        }
      },
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-RunRemoteScript"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSTransform"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation",
        "ssm:GetCommandInvocation"
```

```
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:PutObject",
        "s3:ListMultipartUploadParts",
        "s3:ListBucketMultipartUploads",
        "s3:AbortMultipartUpload",
        "s3:PutBucketTagging"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-transform-deployment-bucket-*",
        "arn:aws:s3:::aws-transform-deployment-bucket-*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
```

```
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedFor" : "AWSTransform",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:EncryptionContext:aws-transform" : "*",
          "kms:ViaService" : "s3.*.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ],
          "kms:EncryptionContext:aws:ebs:id" : "*"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "kms:GrantConstraintType" : "EncryptionContextSubset"
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
```

```
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com",
          "kms:EncryptionContext:aws:ebs:id" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSTransformApplicationECSDeploymentPolicy

説明: AWS Transform が Fargate を使用して Amazon Elastic Container Service (ECS) にアプリケーションをデプロイできるようにします。ECS でアプリケーションを実行するために必要な基盤インフラストラクチャをプロビジョニング、設定、管理するアクセス許可を付与します。

`AWSTransformApplicationECSDeploymentPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSTransformApplicationECSDeploymentPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2025 年 9 月 29 日 22:49 UTC
- 編集日時: 2025 年 11 月 21 日 23:34 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSTransformApplicationECSDeploymentPolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "cloudformation:CreateStack",
      "Resource" : "arn:aws:cloudformation:*:*:stack/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:RequestTag/CreatedBy" : "AWSTransform"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "cloudformation:UpdateStack",
        "cloudformation:DeleteStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CreatedBy" : "AWSTransform"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ecs:CreateCluster",
      "Resource" : "arn:aws:ecs:*:*:cluster/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:RequestTag/CreatedBy" : "AWSTransform"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:UpdateCluster",
        "ecs:DeleteCluster"
      ],
      "Resource" : "arn:aws:ecs:*:*:cluster/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "ecs:ResourceTag/CreatedBy" : "AWSTransform"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ecs:RegisterTaskDefinition",
      "Resource" : "arn:aws:ecs:*:*:task-definition/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:RequestTag/CreatedBy" : "AWSTransform"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ecs:RunTask",
      "Resource" : "arn:aws:ecs:*:*:task-definition/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CreatedBy" : "AWSTransform"
        },
        "ArnLike" : {
          "ecs:cluster" : "arn:aws:ecs:*:*:cluster/AWSTransform*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ecs:ListTasks",
      "Resource" : "arn:aws:ecs:*:*:container-instance/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ArnLike" : {
          "ecs:cluster" : "arn:aws:ecs:*:*:cluster/AWSTransform*"
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : "ecs:DescribeTasks",
      "Resource" : "arn:aws:ecs:*:*:task/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ArnLike" : {
          "ecs:cluster" : "arn:aws:ecs:*:*:cluster/AWSTransform*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/AWSTransform-Deploy-ECS-Task-Role",
        "arn:aws:iam::*:role/AWSTransform-Deploy-ECS-Execution-Role"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "iam:PassedToService" : [
            "ecs-tasks.amazonaws.com",
            "ecs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSTransform-Deploy-ECS-Task-Role",
        "arn:aws:iam::*:role/AWSTransform-Deploy-ECS-Execution-Role"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ecs:CreateService",
      "Resource" : "arn:aws:ecs:*:*:service/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:RequestTag/CreatedBy" : "AWSTransform"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:UpdateService",
        "ecs:DeleteService"
      ],
      "Resource" : "arn:aws:ecs:*:*:service/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "ecs:ResourceTag/CreatedBy" : "AWSTransform"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:cluster/AWSTransform*",
        "arn:aws:ecs:*:*:task-definition/AWSTransform*",
        "arn:aws:ecs:*:*:service/AWSTransform*",
        "arn:aws:ecs:*:*:task/AWSTransform*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
```

```
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "ResourceName",
            "CreatedBy",
            "TransformationType"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:TagResource"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/ecs/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:RequestTag/CreatedBy" : "AWSTransform"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "ResourceName",
            "CreatedBy",
            "TransformationType"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DeleteLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/ecs/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : "logs:UntagResource",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/ecs/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "ResourceName",
            "CreatedBy",
            "TransformationType"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:GetLogEvents",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/ecs/AWSTransform*:log-stream:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository",
        "ecr:TagResource"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/awstransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:RequestTag/CreatedBy" : "AWSTransform"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "ResourceName",
            "CreatedBy",
            "TransformationType"
          ]
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeClusters",
        "ecs:DescribeServices",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeNetworkInterfaces",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/ecs.amazonaws.com/
AWSServiceRoleForECS",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ecs.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "ecr.*.amazonaws.com"
          ],
          "kms:EncryptionContext:aws:ecr:arn" : "*"
```

```
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "kms:GrantConstraintType" : "EncryptionContextSubset"
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt",
            "GenerateDataKey"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSTransformCustomExecuteTransformations

説明: AWS Transform custom で変換を実行するためのアクセスを提供します。

`AWSTransformCustomExecuteTransformations` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSTransformCustomExecuteTransformations` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 12 月 5 日 15:34 UTC

- 編集日時: 2025 年 12 月 5 日 15:34 UTC
- ARN: arn:aws:iam::aws:policy/AWSTransformCustomExecuteTransformations

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSTransformCustomExecuteTransformations",
      "Effect" : "Allow",
      "Action" : [
        "transform-custom:ConverseStream",
        "transform-custom:ExecuteTransformation",
        "transform-custom:GetCampaign",
        "transform-custom:UpdateCampaignRepositoryStatus",
        "transform-custom:UpdateCampaign"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSTransformCustomFullAccess

説明: AWS Transform custom へのフルアクセスを提供します。

AWSTransformCustomFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSTransformCustomFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 12 月 5 日 15:19 UTC
- 編集日時: 2025 年 12 月 5 日 15:19 UTC
- ARN: arn:aws:iam::aws:policy/AWSTransformCustomFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSTransformCustomAllActions",
      "Effect" : "Allow",
      "Action" : [
        "transform-custom:*"
      ],
      "Resource" : [
        "*"
      ]
```

```
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSTransformCustomManageTransformations

説明: AWS Transform custom で変換リソースの管理と変換の実行を有効にします。

`AWSTransformCustomManageTransformations` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSTransformCustomManageTransformations` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 12 月 5 日 15:49 UTC
- 編集日時: 2025 年 12 月 5 日 15:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransformCustomManageTransformations`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSTransformCustomManageTransformations",
      "Effect" : "Allow",
      "Action" : [
        "transform-custom:ConverseStream",
        "transform-custom:CreateTransformationPackageUrl",
        "transform-custom:CompleteTransformationPackageUpload",
        "transform-custom:DeleteTransformationPackage",
        "transform-custom:GetTransformationPackageUrl",
        "transform-custom:ListTransformationPackageMetadata",
        "transform-custom:ExecuteTransformation",
        "transform-custom:ListKnowledgeItems",
        "transform-custom:GetKnowledgeItem",
        "transform-custom:DeleteKnowledgeItem",
        "transform-custom:UpdateKnowledgeItemConfiguration",
        "transform-custom:UpdateKnowledgeItemStatus",
        "transform-custom:GetCampaign",
        "transform-custom:UpdateCampaignRepositoryStatus",
        "transform-custom:UpdateCampaign",
        "transform-custom:ListTagsForResource",
        "transform-custom:TagResource",
        "transform-custom:UntagResource"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSTrustedAdvisorPriorityFullAccess

説明: AWS Trusted Advisor Priority へのフルアクセスを提供します。このポリシーにより、ユーザーは Trusted Advisor を AWS Organizations の信頼されたサービスとして追加し、Trusted Advisor Priority の委任管理者アカウントを指定することもできます。

AWSTrustedAdvisorPriorityFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSTrustedAdvisorPriorityFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 8 月 16 日 16:08 UTC
- 編集日時: 2022 年 8 月 16 日 16:08 UTC
- ARN: arn:aws:iam::aws:policy/AWSTrustedAdvisorPriorityFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSTrustedAdvisorPriorityReadOnlyAccess

説明: AWS Trusted Advisor Priority への読み取り専用アクセスを提供します。これには、委任管理者アカウントを閲覧する許可が含まれます。

`AWSTrustedAdvisorPriorityReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSTrustedAdvisorPriorityReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2022 年 8 月 16 日 16:35 UTC
- 編集日時: 2022 年 8 月 16 日 16:35 UTC
- ARN: arn:aws:iam::aws:policy/AWSTrustedAdvisorPriorityReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSTrustedAdvisorReportingServiceRolePolicy

説明: Trusted Advisor マルチアカウントレポートのサービスポリシー

`AWSTrustedAdvisorReportingServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 11 月 19 日 17:41 UTC
- 編集日時: 2023 年 2 月 28 日 23:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSTrustedAdvisorReportingServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSTrustedAdvisorServiceRolePolicy

説明: コストを削減し、パフォーマンスを向上させ、 AWS 環境のセキュリティを向上させるために、 AWS Trusted Advisor Service へのアクセス。

AWSTrustedAdvisorServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 2 月 22 日 21:24 UTC
- 編集日時: 2024 年 10 月 30 日 16:52 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSTrustedAdvisorServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v14 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TrustedAdvisorServiceRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:ListAnalyzers",
```

```
        "autoscaling:DescribeAccountLimits",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeLaunchConfigurations",
        "ce:GetReservationPurchaseRecommendation",
        "ce:GetSavingsPlansPurchaseRecommendation",
        "cloudformation:DescribeAccountLimits",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks",
        "cloudfront:ListDistributions",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:GetTrail",
        "cloudtrail:ListTrails",
        "cloudtrail:GetEventSelectors",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "dax:DescribeClusters",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeTable",
        "dynamodb:ListTables",
        "ec2:DescribeAddresses",
        "ec2:DescribeReservedInstances",
        "ec2:DescribeInstances",
        "ec2:DescribeVpcs",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeImages",
        "ec2:DescribeNatGateways",
        "ec2:DescribeVolumes",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeRegions",
        "ec2:DescribeReservedInstancesOfferings",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:GetManagedPrefixListEntries",
        "ecs:DescribeTaskDefinition",
        "ecs:ListTaskDefinitions",
        "elasticloadbalancing:DescribeAccountLimits",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
```

```
        "elasticloadbalancing:DescribeLoadBalancerPolicies",
        "elasticloadbalancing:DescribeLoadBalancerPolicyTypes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "iam:GenerateCredentialReport",
        "iam:GetAccountPasswordPolicy",
        "iam:GetAccountSummary",
        "iam:GetCredentialReport",
        "iam:GetServerCertificate",
        "iam:ListServerCertificates",
        "iam:ListSAMLProviders",
        "kinesis:DescribeLimits",
        "kafka:DescribeClusterV2",
        "kafka:ListClustersV2",
        "kafka:ListNodes",
        "network-firewall:ListFirewalls",
        "network-firewall:DescribeFirewall",
        "outposts:ListAssets",
        "outposts:GetOutpost",
        "outposts:ListOutposts",
        "rds:DescribeAccountAttributes",
        "rds:DescribeDBClusters",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBSnapshots",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultParameters",
        "rds:DescribeEvents",
        "rds:DescribeOptionGroupOptions",
        "rds:DescribeOptionGroups",
        "rds:DescribeOrderableDBInstanceOptions",
        "rds:DescribeReservedDBInstances",
        "rds:DescribeReservedDBInstancesOfferings",
        "rds:ListTagsForResource",
        "redshift:DescribeClusters",
        "redshift:DescribeReservedNodeOfferings",
        "redshift:DescribeReservedNodes",
        "route53:GetAccountLimit",
```

```
        "route53:GetHealthCheck",
        "route53:GetHostedZone",
        "route53:ListHealthChecks",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName",
        "route53:ListResourceRecordSets",
        "route53resolver:ListResolverEndpoints",
        "route53resolver:ListResolverEndpointIpAddresses",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketVersioning",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetLifecycleConfiguration",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "ses:GetSendQuota",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSUserAttributeCostAllocationPolicy

説明: 顧客がオプトインしたユーザー属性に対して、IAM Identity Center AWS からのユーザー属性への読み取り専用アクセスを提供します。

`AWSUserAttributeCostAllocationPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2025 年 12 月 15 日 16:34 UTC
- 編集日時: 2025 年 12 月 15 日 16:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSUserAttributeCostAllocationPolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/user-attribute-cost-allocation-data.amazonaws.com/AWSServiceRoleForUserAttributeCostAllocation"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する

- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSUserNotificationsServiceLinkedRolePolicy

説明: AWS ユーザー通知がユーザーに代わって AWS サービスを呼び出すことを許可します。

AWSUserNotificationsServiceLinkedRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 4 月 19 日 13:28 UTC
- 編集日時: 2025 年 9 月 2 日 20:49 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSUserNotificationsServiceLinkedRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
```

```
        "events:PutRule",
        "events:PutTargets",
        "events:DeleteRule",
        "events:ListTargetsByRule",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/AWSUserNotificationsManagedRule-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Notifications"
        }
      },
      "Resource" : "*"
    },
    {
      "Sid" : "AllowOrgsActions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListChildren",
        "organizations:ListParents"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationsAdminDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
```

```
            "notifications.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "OrganizationNotificationConfigurationDistribution",
      "Effect" : "Allow",
      "Action" : [
        "notifications:CreateNotificationConfiguration",
        "notifications:DeleteNotificationConfiguration",
        "notifications:CreateEventRule",
        "notifications:UpdateEventRule",
        "notifications:DeleteEventRule"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSVendorInsightsAssessorFullAccess

説明: 資格のある Vendor Insights リソースを閲覧し、Vendor Insights サブスクリプションを管理するためのフルアクセスを提供します。

`AWSVendorInsightsAssessorFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSVendorInsightsAssessorFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2022 年 7 月 26 日 15:05 UTC
- 編集日時: 2022 年 12 月 1 日 00:51 UTC
- ARN: arn:aws:iam::aws:policy/AWSVendorInsightsAssessorFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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/*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSVendorInsightsAssessorReadOnly

説明: 資格のある Vendor Insights リソースを閲覧するための読み取り専用アクセスを提供します

`AWSVendorInsightsAssessorReadOnly` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSVendorInsightsAssessorReadOnly` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 7 月 26 日 15:05 UTC

- 編集日時: 2022 年 12 月 1 日 00:55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSVendorInsightsAssessorReadOnly`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する

- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSVendorInsightsVendorFullAccess

説明: Vendor Insights リソースの作成および管理のためのフルアクセスを提供します

AWSVendorInsightsVendorFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSVendorInsightsVendorFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 7 月 26 日 15:05 UTC
- 編集日時: 2023 年 10 月 19 日 01:41 UTC
- ARN: arn:aws:iam::aws:policy/AWSVendorInsightsVendorFullAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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/*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSVendorInsightsVendorReadOnly

説明: Vendor Insights リソースを閲覧するための読み取り専用アクセスを提供します

AWSVendorInsightsVendorReadOnly は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSVendorInsightsVendorReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2022 年 7 月 26 日 15:05 UTC
- 編集日時: 2022 年 12 月 1 日 00:54 UTC
- ARN: arn:aws:iam::aws:policy/AWSVendorInsightsVendorReadOnly

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSVpcLatticeServiceRolePolicy

説明: VPC Lattice がユーザーに代わって AWS リソースにアクセスできるようにします。

AWSVpcLatticeServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 11 月 30 日 20:47 UTC
- 編集日時: 2024 年 12 月 1 日 14:06 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSVpcLatticeServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/VpcLattice"
        }
      }
    },
    {
      "Sid" : "VpcLatticeDescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VpcLatticeCreateNetworkInterfaceWithTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:RequestTag/VpcLatticeManaged" : "true"
        }
      }
    },
    {
      "Sid" : "VpcLatticeCreateNetworkInterfaceWithSubnetAndSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "VpcLatticeTagNetworkInterfaceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        }
      }
    },
    {
      "Sid" : "VpcLatticeMutateNetworkInterfaceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/VpcLatticeManaged" : "true"
        }
      }
    },
    {
```

```
      "Sid" : "VpcLatticeModifyNetworkInterfaceSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*"
    },
    {
      "Sid" : "VpcLatticeModifyNetworkInterfaceActionsIpAddressActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignIpv6Addresses",
        "ec2:UnassignIpv6Addresses",
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/VpcLatticeManaged" : "true"
        }
      }
    },
    {
      "Sid" : "VpcLatticeAssociateHostedZoneToVpc",
      "Effect" : "Allow",
      "Action" : [
        "route53:AssociateVPCWithHostedZone"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSVPCS2SVpnServiceRolePolicy

説明: Site-to-Site VPN が、お使いの VPN 接続に関連するリソースを作成および管理できるようにします。

AWSVPCS2SVpnServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 8 月 6 日 14:13 UTC
- 編集日時: 2025 年 5 月 15 日 16:52 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSVPCS2SVpnServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "0",
      "Effect" : "Allow",
      "Action" : [
```

```
        "acm:ExportCertificate",
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "acm-pca:DescribeCertificateAuthority"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VpnConnectionSecretsManagement",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:PutSecretValue",
        "secretsmanager:UpdateSecret",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:s2svpn!*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "s2svpn",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "VpnConnectionSecretsCreation",
      "Effect" : "Allow",
      "Action" : "secretsmanager:CreateSecret",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:s2svpn!*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:Name" : "s2svpn!*"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSVPCTransitGatewayServiceRolePolicy

説明: VPC Transit ゲートウェイ が Transit ゲートウェイ VPC アタッチメント向けに必要なリソースを作成および管理できるようにします。

AWSVPCTransitGatewayServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 11 月 26 日 16:21 UTC
- 編集日時: 2021 年 4 月 15 日 16:31 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSVPCTransitGatewayServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSVPCVerifiedAccessServiceRolePolicy

説明: AWS Verified Access サービスがユーザーに代わってエンドポイントをプロビジョニングできるようにするポリシー

AWSVPCVerifiedAccessServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 11 月 29 日 03:35 UTC
- 編集日時: 2023 年 11 月 17 日 21:03 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSVPCVerifiedAccessServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSWAFConsoleFullAccess

説明: 経由で AWS WAF へのフルアクセスを提供します AWS マネジメントコンソール。このポリシーは、Amazon CloudFront ディストリビューションを一覧表示および更新するアクセス許可、

AWS Elastic Load Balancing でロードバランサーを表示するアクセス許可、Amazon API Gateway REST APIs およびステージを表示するアクセス許可、Amazon CloudWatch メトリクスを一覧表示および表示するアクセス許可、アカウント内で有効になっているリージョンを表示するアクセス許可も付与することに注意してください。

AWSWAFConsoleFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSWAFConsoleFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 4 月 6 日 18:38 UTC
- 編集日時: 2025 年 11 月 19 日 02:34 UTC
- ARN: arn:aws:iam::aws:policy/AWSWAFConsoleFullAccess

ポリシーのバージョン

ポリシーのバージョン: v12 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowUseOfAWSWAFClassic",
      "Effect" : "Allow",
      "Action" : [
        "waf:*",
        "waf-regional:*"
      ],
      "Resource" : [
        "arn:aws:waf::*:bytematchset/*",
```

```
        "arn:aws:waf::*:ipset/*",
        "arn:aws:waf::*:ratebasedrule/*",
        "arn:aws:waf::*:rule/*",
        "arn:aws:waf::*:sizeconstraintset/*",
        "arn:aws:waf::*:sqlinjectionset/*",
        "arn:aws:waf::*:webacl/*",
        "arn:aws:waf::*:xssmatchset/*",
        "arn:aws:waf::*:regexmatch/*",
        "arn:aws:waf::*:regexpatternset/*",
        "arn:aws:waf::*:geomatchset/*",
        "arn:aws:waf::*:rulegroup/*",
        "arn:aws:waf:*:*:changetoken/*",
        "arn:aws:waf-regional:*:*:bytematchset/*",
        "arn:aws:waf-regional:*:*:ipset/*",
        "arn:aws:waf-regional:*:*:ratebasedrule/*",
        "arn:aws:waf-regional:*:*:rule/*",
        "arn:aws:waf-regional:*:*:sizeconstraintset/*",
        "arn:aws:waf-regional:*:*:sqlinjectionset/*",
        "arn:aws:waf-regional:*:*:webacl/*",
        "arn:aws:waf-regional:*:*:xssmatchset/*",
        "arn:aws:waf-regional:*:*:regexmatch/*",
        "arn:aws:waf-regional:*:*:regexpatternset/*",
        "arn:aws:waf-regional:*:*:geomatchset/*",
        "arn:aws:waf-regional:*:*:rulegroup/*",
        "arn:aws:waf-regional:*:*:changetoken/*"
      ]
    },
    {
      "Sid" : "AllowWAFClassicGetWebACLForResource",
      "Effect" : "Allow",
      "Action" : [
        "waf-regional:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:waf-regional:*:*:*/*"
    },
    {
      "Sid" : "AllowUseOfAWSWAF",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:*"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:*/webacl/*/*",
        "arn:aws:wafv2:*:*:*/ipset/*/*",
```

```
        "arn:aws:wafv2:*:*:*/managedruleset/*/*",
        "arn:aws:wafv2:*:*:*/rulegroup/*/*",
        "arn:aws:wafv2:*:*:*/regexpatternset/*/*"
      ]
    },
    {
      "Sid" : "AllowDisassociateWebACL",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:DisassociateWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowS3ListAllMyBuckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowEC2DescribeRegions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeRegions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowListActionsForCloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForCloudFront",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:GetDistributionConfig",
```

```
        "cloudfront:GetDistribution",
        "cloudfront:UpdateDistribution",
        "cloudfront:AssociateDistributionWebACL",
        "cloudfront:DisassociateDistributionWebACL"
      ],
      "Resource" : "arn:aws:cloudfront::*:distribution/*"
    },
    {
      "Sid" : "AllowListActionsForCloudFront",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:ListDistributions",
        "cloudfront:ListDistributionsByWebACLId"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForCloudFrontTenant",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:GetDistributionTenant",
        "cloudfront:AssociateDistributionTenantWebACL",
        "cloudfront:DisassociateDistributionTenantWebACL"
      ],
      "Resource" : "arn:aws:cloudfront::*:distribution-tenant/*"
    },
    {
      "Sid" : "AllowListActionsForCloudFrontTenant",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:ListDistributionTenants",
        "cloudfront:ListDistributionTenantsByCustomization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForALB",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:SetWebAcl"
      ],
      "Resource" : "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*"
    },
    {
```

```
      "Sid" : "AllowListActionsForALB",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForAPIGateway",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:SetWebACL"
      ],
      "Resource" : "arn:aws:apigateway:*::/restapis/*/stages/*"
    },
    {
      "Sid" : "AllowListActionsForAPIGateway",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : "arn:aws:apigateway:*::/*"
    },
    {
      "Sid" : "AllowActionsForAppSync",
      "Effect" : "Allow",
      "Action" : [
        "appsync:SetWebACL"
      ],
      "Resource" : "arn:aws:appsync:*:*:apis/*"
    },
    {
      "Sid" : "AllowListActionsForAppSync",
      "Effect" : "Allow",
      "Action" : [
        "appsync:ListGraphqlApis",
        "appsync:ListApis"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForCognito",
      "Effect" : "Allow",
      "Action" : [
```

```
        "cognito-idp:AssociateWebACL",
        "cognito-idp:DisassociateWebACL",
        "cognito-idp:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:cognito-idp:*:*:userpool/*"
    },
    {
      "Sid" : "AllowListActionsForCognito",
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:ListUserPools",
        "cognito-idp:ListResourcesForWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForAppRunner",
      "Effect" : "Allow",
      "Action" : [
        "apprunner:AssociateWebAcl",
        "apprunner:DisassociateWebAcl",
        "apprunner:DescribeWebAclForService"
      ],
      "Resource" : "arn:aws:apprunner:*:*:service/*/*"
    },
    {
      "Sid" : "AllowListActionsForAppRunner",
      "Effect" : "Allow",
      "Action" : [
        "apprunner:ListServices",
        "apprunner:ListAssociatedServicesForWebAcl"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForAVA",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateVerifiedAccessInstanceWebAcl",
        "ec2:DisassociateVerifiedAccessInstanceWebAcl",
        "ec2:GetVerifiedAccessInstanceWebAcl"
      ],
      "Resource" : "arn:aws:ec2:*:*:verified-access-instance/*"
    },
```

```
    {
      "Sid" : "AllowListActionsForAVA",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVerifiedAccessInstances",
        "ec2:DescribeVerifiedAccessInstanceWebAclAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForAmplify",
      "Effect" : "Allow",
      "Action" : [
        "amplify:AssociateWebACL",
        "amplify:DisassociateWebACL",
        "amplify:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:amplify:*:*:apps/*"
    },
    {
      "Sid" : "AllowListActionsForAmplify",
      "Effect" : "Allow",
      "Action" : [
        "amplify:ListApps",
        "amplify:ListResourcesForWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowLogQueryActions",
      "Effect" : "Allow",
      "Action" : [
        "logs:StartQuery",
        "logs:DescribeQueryDefinitions",
        "logs:GetQueryResults"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:aws-waf-logs-*"
    },
    {
      "Sid" : "AllowLogGroupDescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowLogDeliverySubscription",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:DeleteLogDelivery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GrantLogDeliveryPermissionForS3Bucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketPolicy",
        "s3:GetBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-waf-logs-*"
      ]
    },
    {
      "Sid" : "GrantLogDeliveryPermissionForCloudWatchLogGroup",
      "Effect" : "Allow",
      "Action" : [
        "logs:PutResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "wafv2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowListActionForFirehoseStream",
      "Effect" : "Allow",
      "Action" : [
        "firehose:ListDeliveryStreams"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForPricing",
      "Effect" : "Allow",
      "Action" : [
        "pricing:ListPriceLists",
        "pricing:GetPriceListFileUrl"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowMarketplaceViewSubscriptions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ViewSubscriptions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForPricingPlanManager",
      "Effect" : "Allow",
      "Action" : [
        "pricingplanmanager:GetSubscription",
        "pricingplanmanager:UpdateSubscription",
        "pricingplanmanager:CancelSubscription",
        "pricingplanmanager:CancelSubscriptionChange"
      ],
      "Resource" : "arn:aws:pricingplanmanager::*:subscription:*"
    },
    {
      "Sid" : "AllowListActionsForRoute53",
      "Effect" : "Allow",
      "Action" : [
        "route53:ListHostedZones",
        "route53:GetHostedZone"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowListActionsForPricingPlanManager",
      "Effect" : "Allow",
      "Action" : "pricingplanmanager:ListSubscriptions",
      "Resource" : "*"
```

```
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSWAFConsoleReadOnlyAccess

説明: 経由で AWS WAF への読み取り専用アクセスを提供します AWS マネジメントコンソール。このポリシーは、Amazon CloudFront ディストリビューションを一覧表示するアクセス許可、 AWS Elastic Load Balancing でロードバランサーを表示するアクセス許可、Amazon API Gateway REST APIs とステージを表示するアクセス許可、Amazon CloudWatch メトリクスを一覧表示および表示するアクセス許可、およびアカウント内で有効になっているリージョンを表示するアクセス許可も付与することに注意してください。

`AWSWAFConsoleReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSWAFConsoleReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 4 月 6 日 18:43 UTC
- 編集日時: 2025 年 11 月 19 日 02:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWAFConsoleReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v11 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadOnlyOfAWSWAFClassic",
      "Effect" : "Allow",
      "Action" : [
        "waf:Get*",
        "waf:List*",
        "waf-regional:Get*",
        "waf-regional:List*"
      ],
      "Resource" : [
        "arn:aws:waf::*:bytematchset/*",
        "arn:aws:waf::*:ipset/*",
        "arn:aws:waf::*:ratebasedrule/*",
        "arn:aws:waf::*:rule/*",
        "arn:aws:waf::*:sizeconstraintset/*",
        "arn:aws:waf::*:sqlinjectionset/*",
        "arn:aws:waf::*:webacl/*",
        "arn:aws:waf::*:xssmatchset/*",
        "arn:aws:waf::*:regexmatch/*",
        "arn:aws:waf::*:regexpatternset/*",
        "arn:aws:waf::*:geomatchset/*",
        "arn:aws:waf::*:rulegroup/*",
        "arn:aws:waf:*:*:changetoken/*",
        "arn:aws:waf-regional:*:*:bytematchset/*",
        "arn:aws:waf-regional:*:*:ipset/*",
        "arn:aws:waf-regional:*:*:ratebasedrule/*",
        "arn:aws:waf-regional:*:*:rule/*",
        "arn:aws:waf-regional:*:*:sizeconstraintset/*",
        "arn:aws:waf-regional:*:*:sqlinjectionset/*",
        "arn:aws:waf-regional:*:*:webacl/*",
        "arn:aws:waf-regional:*:*:xssmatchset/*",
        "arn:aws:waf-regional:*:*:regexmatch/*",
        "arn:aws:waf-regional:*:*:regexpatternset/*",
        "arn:aws:waf-regional:*:*:geomatchset/*",
```

```
        "arn:aws:waf-regional:*:*:rulegroup/*",
        "arn:aws:waf-regional:*:*:changetoken/*"
      ]
    },
    {
      "Sid" : "AllowWAFClassicGetWebACLForResource",
      "Effect" : "Allow",
      "Action" : [
        "waf-regional:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:waf-regional:*:*:*/*"
    },
    {
      "Sid" : "AllowReadOnlyOfAWSWAF",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:Get*",
        "wafv2:List*",
        "wafv2:Describe*",
        "wafv2:CheckCapacity"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:*/webacl/*/*",
        "arn:aws:wafv2:*:*:*/ipset/*/*",
        "arn:aws:wafv2:*:*:*/managedruleset/*/*",
        "arn:aws:wafv2:*:*:*/rulegroup/*/*",
        "arn:aws:wafv2:*:*:*/regexpatternset/*/*"
      ]
    },
    {
      "Sid" : "AllowEC2DescribeRegions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeRegions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowListActionsForCloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionForCloudFront",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:GetDistributionConfig",
        "cloudfront:GetDistribution"
      ],
      "Resource" : "arn:aws:cloudfront::*:distribution/*"
    },
    {
      "Sid" : "AllowListActionsForCloudFront",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:ListDistributions",
        "cloudfront:ListDistributionsByWebACLId"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionForCloudFrontTenant",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:GetDistributionTenant"
      ],
      "Resource" : "arn:aws:cloudfront::*:distribution-tenant/*"
    },
    {
      "Sid" : "AllowListActionsForCloudFrontTenant",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:ListDistributionTenants",
        "cloudfront:ListDistributionTenantsByCustomization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowListActionsForALB",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "AllowListActionsForAPIGateway",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : "arn:aws:apigateway:*::/*"
    },
    {
      "Sid" : "AllowListActionsForAppSync",
      "Effect" : "Allow",
      "Action" : [
        "appsync:ListGraphqlApis",
        "appsync:ListApis"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionForCognito",
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:cognito-idp:*:*:userpool/*"
    },
    {
      "Sid" : "AllowListActionsForCognito",
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:ListUserPools",
        "cognito-idp:ListResourcesForWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionForAppRunner",
      "Effect" : "Allow",
      "Action" : [
        "apprunner:DescribeWebAclForService"
      ],
      "Resource" : "arn:aws:apprunner:*:*:service/*/*"
    },
```

```
    {
      "Sid" : "AllowListActionsForAppRunner",
      "Effect" : "Allow",
      "Action" : [
        "apprunner:ListServices",
        "apprunner:ListAssociatedServicesForWebAcl"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionForAVA",
      "Effect" : "Allow",
      "Action" : [
        "ec2:GetVerifiedAccessInstanceWebAcl"
      ],
      "Resource" : "arn:aws:ec2:*:*:verified-access-instance/*"
    },
    {
      "Sid" : "AllowListActionsForAVA",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVerifiedAccessInstances",
        "ec2:DescribeVerifiedAccessInstanceWebAclAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionForAmplify",
      "Effect" : "Allow",
      "Action" : [
        "amplify:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:amplify:*:*:apps/*"
    },
    {
      "Sid" : "AllowListActionsForAmplify",
      "Effect" : "Allow",
      "Action" : [
        "amplify:ListApps",
        "amplify:ListResourcesForWebACL"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "AllowS3ListAllMyBuckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowLogGroupDescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowListActionForFirehoseStream",
      "Effect" : "Allow",
      "Action" : [
        "firehose:ListDeliveryStreams"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForPricing",
      "Effect" : "Allow",
      "Action" : [
        "pricing:ListPriceLists",
        "pricing:GetPriceListFileUrl"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowMarketplaceViewSubscriptions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ViewSubscriptions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowLogQueryActions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "logs:StartQuery",
        "logs:DescribeQueryDefinitions",
        "logs:GetQueryResults"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:aws-waf-logs-*"
    },
    {
      "Sid" : "AllowListActionsForPricingPlanManager",
      "Effect" : "Allow",
      "Action" : [
        "pricingplanmanager:GetSubscription"
      ],
      "Resource" : "arn:aws:pricingplanmanager::*:subscription:*"
    },
    {
      "Sid" : "AllowListActionsForRoute53",
      "Effect" : "Allow",
      "Action" : [
        "route53:ListHostedZones",
        "route53:GetHostedZone"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowListSubscriptionsForPricingPlanManager",
      "Effect" : "Allow",
      "Action" : [
        "pricingplanmanager:ListSubscriptions"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSWAFFullAccess

説明: AWS WAF アクションへのフルアクセスを提供します。

AWSWAFFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSWAFFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 10 月 6 日 20:44 UTC
- 編集日時: 2025 年 5 月 5 日 21:07 UTC
- ARN: arn:aws:iam::aws:policy/AWSWAFFullAccess

ポリシーのバージョン

ポリシーのバージョン: v12 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowUseOfAWSWAFClassic",
      "Effect" : "Allow",
      "Action" : [
        "waf:*",
        "waf-regional:*"
      ],
      "Resource" : [
        "arn:aws:waf::*:bytematchset/*",
        "arn:aws:waf::*:ipset/*",
```

```
        "arn:aws:waf::*:ratebasedrule/*",
        "arn:aws:waf::*:rule/*",
        "arn:aws:waf::*:sizeconstraintset/*",
        "arn:aws:waf::*:sqlinjectionset/*",
        "arn:aws:waf::*:webacl/*",
        "arn:aws:waf::*:xssmatchset/*",
        "arn:aws:waf::*:regexmatch/*",
        "arn:aws:waf::*:regexpatternset/*",
        "arn:aws:waf::*:geomatchset/*",
        "arn:aws:waf::*:rulegroup/*",
        "arn:aws:waf::*:changetoken/*",
        "arn:aws:waf-regional:*:*:bytematchset/*",
        "arn:aws:waf-regional:*:*:ipset/*",
        "arn:aws:waf-regional:*:*:ratebasedrule/*",
        "arn:aws:waf-regional:*:*:rule/*",
        "arn:aws:waf-regional:*:*:sizeconstraintset/*",
        "arn:aws:waf-regional:*:*:sqlinjectionset/*",
        "arn:aws:waf-regional:*:*:webacl/*",
        "arn:aws:waf-regional:*:*:xssmatchset/*",
        "arn:aws:waf-regional:*:*:regexmatch/*",
        "arn:aws:waf-regional:*:*:regexpatternset/*",
        "arn:aws:waf-regional:*:*:geomatchset/*",
        "arn:aws:waf-regional:*:*:rulegroup/*",
        "arn:aws:waf-regional:*:*:changetoken/*"
      ]
    },
    {
      "Sid" : "AllowWAFClassicGetWebACLForResource",
      "Effect" : "Allow",
      "Action" : [
        "waf-regional:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:waf-regional:*:*:*/*"
    },
    {
      "Sid" : "AllowUseOfAWSWAF",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:*"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:*/webacl/*/*",
        "arn:aws:wafv2:*:*:*/ipset/*/*",
        "arn:aws:wafv2:*:*:*/managedruleset/*/*",
```

```
        "arn:aws:wafv2:*:*:*/rulegroup/*/*",
        "arn:aws:wafv2:*:*:*/regexpatternset/*/*"
      ]
    },
    {
      "Sid" : "AllowDisassociateWebACL",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:DisassociateWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForALB",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:SetWebAcl"
      ],
      "Resource" : "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*"
    },
    {
      "Sid" : "AllowActionsForAPIGateway",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:SetWebACL"
      ],
      "Resource" : "arn:aws:apigateway:*::/restapis/*/stages/*"
    },
    {
      "Sid" : "AllowActionsForAppSync",
      "Effect" : "Allow",
      "Action" : [
        "appsync:SetWebACL"
      ],
      "Resource" : "arn:aws:appsync:*:*:apis/*"
    },
    {
      "Sid" : "AllowActionsForCognito",
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:AssociateWebACL",
        "cognito-idp:DisassociateWebACL",
        "cognito-idp:GetWebACLForResource"
      ],
```

```
      "Resource" : "arn:aws:cognito-idp:*:*:userpool/*"
    },
    {
      "Sid" : "AllowListActionsForCognito",
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:ListResourcesForWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForAppRunner",
      "Effect" : "Allow",
      "Action" : [
        "apprunner:AssociateWebAcl",
        "apprunner:DisassociateWebAcl",
        "apprunner:DescribeWebAclForService"
      ],
      "Resource" : "arn:aws:apprunner:*:*:service/*/*"
    },
    {
      "Sid" : "AllowListActionsForAppRunner",
      "Effect" : "Allow",
      "Action" : [
        "apprunner:ListServices",
        "apprunner:ListAssociatedServicesForWebAcl"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForAVA",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateVerifiedAccessInstanceWebAcl",
        "ec2:DisassociateVerifiedAccessInstanceWebAcl",
        "ec2:GetVerifiedAccessInstanceWebAcl"
      ],
      "Resource" : "arn:aws:ec2:*:*:verified-access-instance/*"
    },
    {
      "Sid" : "AllowListActionsForAVA",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVerifiedAccessInstanceWebAclAssociations"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForAmplify",
      "Effect" : "Allow",
      "Action" : [
        "amplify:AssociateWebACL",
        "amplify:DisassociateWebACL",
        "amplify:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:amplify:*:*:apps/*"
    },
    {
      "Sid" : "AllowListActionsForAmplify",
      "Effect" : "Allow",
      "Action" : [
        "amplify:ListResourcesForWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowLogGroupDescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowLogDeliverySubscription",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:DeleteLogDelivery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GrantLogDeliveryPermissionForS3Bucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketPolicy",
```

```
        "s3:GetBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-waf-logs-*"
      ]
    },
    {
      "Sid" : "GrantLogDeliveryPermissionForCloudWatchLogGroup",
      "Effect" : "Allow",
      "Action" : [
        "logs:PutResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "wafv2.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSWAFReadOnlyAccess

説明: AWS WAF アクションへの読み取り専用アクセスを提供します。

AWSWAFReadOnlyAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSWAFReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 10 月 6 日 20:43 UTC
- 編集日時: 2025 年 5 月 5 日 21:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWAFReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v9 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadOnlyOfAWSWAFClassic",
      "Effect" : "Allow",
      "Action" : [
        "waf:Get*",
        "waf:List*",
        "waf-regional:Get*",
        "waf-regional:List*"
      ],
      "Resource" : [
        "arn:aws:waf::*:bytematchset/*",
        "arn:aws:waf::*:ipset/*",
        "arn:aws:waf::*:ratebasedrule/*",
        "arn:aws:waf::*:rule/*",
        "arn:aws:waf::*:sizeconstraintset/*",
        "arn:aws:waf::*:sqlinjectionset/*",
        "arn:aws:waf::*:webacl/*",
        "arn:aws:waf::*:xssmatchset/*",
        "arn:aws:waf::*:regexmatch/*",
        "arn:aws:waf::*:regexpatternset/*",
```

```
        "arn:aws:waf::*:geomatchset/*",
        "arn:aws:waf::*:rulegroup/*",
        "arn:aws:waf::*:changetoken/*",
        "arn:aws:waf-regional:*:*:bytematchset/*",
        "arn:aws:waf-regional:*:*:ipset/*",
        "arn:aws:waf-regional:*:*:ratebasedrule/*",
        "arn:aws:waf-regional:*:*:rule/*",
        "arn:aws:waf-regional:*:*:sizeconstraintset/*",
        "arn:aws:waf-regional:*:*:sqlinjectionset/*",
        "arn:aws:waf-regional:*:*:webacl/*",
        "arn:aws:waf-regional:*:*:xssmatchset/*",
        "arn:aws:waf-regional:*:*:regexmatch/*",
        "arn:aws:waf-regional:*:*:regexpatternset/*",
        "arn:aws:waf-regional:*:*:geomatchset/*",
        "arn:aws:waf-regional:*:*:rulegroup/*",
        "arn:aws:waf-regional:*:*:changetoken/*"
      ]
    },
    {
      "Sid" : "AllowWAFClassicGetWebACLForResource",
      "Effect" : "Allow",
      "Action" : [
        "waf-regional:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:waf-regional:*:*:*/*"
    },
    {
      "Sid" : "AllowReadOnlyOfAWSWAF",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:Get*",
        "wafv2:List*",
        "wafv2:Describe*",
        "wafv2:CheckCapacity"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:*/webacl/*/*",
        "arn:aws:wafv2:*:*:*/ipset/*/*",
        "arn:aws:wafv2:*:*:*/managedruleset/*/*",
        "arn:aws:wafv2:*:*:*/rulegroup/*/*",
        "arn:aws:wafv2:*:*:*/regexpatternset/*/*"
      ]
    },
    {
```

```
      "Sid" : "AllowGetActionForCognito",
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:cognito-idp:*:*:userpool/*"
    },
    {
      "Sid" : "AllowListActionsForCognito",
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:ListResourcesForWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionForAppRunner",
      "Effect" : "Allow",
      "Action" : [
        "apprunner:DescribeWebAclForService"
      ],
      "Resource" : "arn:aws:apprunner:*:*:service/*/*"
    },
    {
      "Sid" : "AllowListActionsForAppRunner",
      "Effect" : "Allow",
      "Action" : [
        "apprunner:ListServices",
        "apprunner:ListAssociatedServicesForWebAcl"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionForAVA",
      "Effect" : "Allow",
      "Action" : [
        "ec2:GetVerifiedAccessInstanceWebAcl"
      ],
      "Resource" : "arn:aws:ec2:*:*:verified-access-instance/*"
    },
    {
      "Sid" : "AllowListActionsForAVA",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:DescribeVerifiedAccessInstanceWebAclAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionForAmplify",
      "Effect" : "Allow",
      "Action" : [
        "amplify:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:amplify:*:*:apps/*"
    },
    {
      "Sid" : "AllowListActionsForAmplify",
      "Effect" : "Allow",
      "Action" : [
        "amplify:ListResourcesForWebACL"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSWellArchitectedDiscoveryServiceRolePolicy

説明: WellArchitected が顧客に代わって WellArchitected リソースに関連する AWS サービスとリソースにアクセスできるようにします。

`AWSWellArchitectedDiscoveryServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 4 月 26 日 18:36 UTC
- 編集日時: 2023 年 4 月 26 日 18:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSWellArchitectedDiscoveryServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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-*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSWellArchitectedOrganizationsServiceRolePolicy

説明: Well-Architected がユーザーに代わって Organizations にアクセスできるようにします。

`AWSWellArchitectedOrganizationsServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 6 月 23 日 17:15 UTC
- 編集日時: 2022 年 7 月 25 日 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSWellArchitectedOrganizationsServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
```

```
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSWickrFullAccess

説明: このポリシーは、 AWS マネジメントコンソールに基づく Wickr 管理機能を含む、Wickr サービスに対する完全な管理者権限をに付与します。

`AWSWickrFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSWickrFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 11 月 27 日 20:36 UTC

- 編集日時: 2022 年 11 月 27 日 20:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWickrFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "wickr:*",
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSXrayCrossAccountSharingConfiguration

説明: オブザーバビリティ Access Manager のリンクを管理し、X-Ray トレースの共有を確立する機能を提供します。

`AWSXrayCrossAccountSharingConfiguration` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSXrayCrossAccountSharingConfiguration をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 11 月 27 日 13:46 UTC
- 編集日時: 2022 年 11 月 27 日 13:46 UTC
- ARN: arn:aws:iam::aws:policy/AWSXrayCrossAccountSharingConfiguration

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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/*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSXRayDaemonWriteAccess

説明: AWS X-Ray デーモンが raw トレースセグメントデータをサービスの API に中継し、X-Ray SDK で使用するサンプリングデータ (ルール、ターゲットなど) を取得できるようにします。

`AWSXRayDaemonWriteAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSXRayDaemonWriteAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 8 月 28 日 23:00 UTC

- 編集日時: 2024 年 2 月 13 日 21:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXRayDaemonWriteAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSXRayDaemonWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSXrayFullAccess

説明: AWS X-Ray フルアクセス管理ポリシー

AWSXrayFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSXrayFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2016 年 12 月 1 日 18:30 UTC
- 編集日時: 2024 年 4 月 11 日 17:07 UTC
- ARN: arn:aws:iam::aws:policy/AWSXrayFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSXrayFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "xray:*"
      ],
      "Resource" : [
        "*"
```

```
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSXrayReadOnlyAccess

説明: AWS X-Ray 読み取り専用管理ポリシー

`AWSXrayReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSXrayReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2016 年 12 月 1 日 18:27 UTC
- 編集日時: 2024 年 2 月 14 日 00:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXrayReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSXrayWriteOnlyAccess

説明: AWS X-Ray 書き込み専用マネージドポリシー

AWSXrayWriteOnlyAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSXrayWriteOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2016 年 12 月 1 日 18:19 UTC
- 編集日時: 2018 年 8 月 28 日 23:03 UTC
- ARN: arn:aws:iam::aws:policy/AWSXrayWriteOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : [
```

```
        "*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

AWSZonalAutoshiftPracticeRunSLRPolicy

説明: ARC ゾーンシフト練習実行の管理アクセスと、練習実行をモニタリングするための CloudWatch アラームステータスへのアクセスを提供します。

`AWSZonalAutoshiftPracticeRunSLRPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 11 月 29 日 17:34 UTC
- 編集日時: 2025 年 6 月 30 日 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSZonalAutoshiftPracticeRunSLRPolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MonitoringPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "health:DescribeEvents"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AutoshiftPracticeCheckPermissions",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAutoScalingGroups",
        "ec2:DescribeInstances",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeTargetGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ZonalShiftManagementPermissions",
      "Effect" : "Allow",
      "Action" : [
        "arc-zonal-shift:CancelZonalShift",
        "arc-zonal-shift:GetManagedResource",
        "arc-zonal-shift:StartZonalShift",
        "arc-zonal-shift:UpdateZonalShift"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSZoneGroupAccessManagementServiceRolePolicy

説明: 組織のゾーングループアクセス管理をサポートするために必要な API への読み取り専用アクセスを提供します。

AWSZoneGroupAccessManagementServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2025 年 7 月 1 日 19:07 UTC
- 編集日時: 2025 年 7 月 1 日 19:07 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSZoneGroupAccessManagementServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Sid" : "AwsOrganizationsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListParents",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListChildren",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

BatchServiceRolePolicy

説明: Amazon EC2 や Amazon ECS リソースなど、必要なリソースを管理するための AWS Batch サービスへのアクセスを提供します。

`BatchServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー

- 作成日時: 2021 年 3 月 10 日 06:55 UTC
- 編集日時: 2023 年 12 月 05 日 22:52 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/BatchServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

BedrockAgentCoreFullAccess

説明: Bedrock AgentCore へのフルアクセスと、関連サービスへの制限付きアクセスを提供します

`BedrockAgentCoreFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `BedrockAgentCoreFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 7 月 16 日 13:37 UTC
- 編集日時: 2025 年 12 月 2 日 13:34 UTC
- ARN: `arn:aws:iam::aws:policy/BedrockAgentCoreFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockAgentCoreFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-agentcore:*"
      ],
      "Resource" : "arn:aws:bedrock-agentcore:*:*:*"
    },
    {
      "Sid" : "IAMListAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:ListRoles"
      ],
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Sid" : "BedrockAgentCorePassRoleAccess",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*BedrockAgentCore*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "bedrock-agentcore.amazonaws.com"
        }
      }
```

```
    },
    {
      "Sid" : "SecretsManagerAccess",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:PutSecretValue",
        "secretsmanager:GetSecretValue",
        "secretsmanager:DeleteSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:bedrock-agentcore*"
    },
    {
      "Sid" : "BedrockAgentCoreKMSReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
        "kms:DescribeKey"
      ],
      "Resource" : [
        "arn:aws:kms:*:*:key/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BedrockAgentCoreKMSAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "kms:ListGrants"
      ],
      "Resource" : [
        "arn:aws:kms:*:*:key/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ForAnyValue:StringEquals" : {
```

```
          "aws:CalledVia" : [
            "bedrock-agentcore.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "BedrockAgentCoreKMSGrantsAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : [
        "arn:aws:kms:*:*:key/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "kms:GrantConstraintType" : "EncryptionContextSubset"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "bedrock-agentcore.*.amazonaws.com"
          ],
          "kms:EncryptionContext:aws:bedrock-agentcore-gateway:arn" : "arn:aws:bedrock-
agentcore:*:*:gateway/*"
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt",
            "GenerateDataKey"
          ]
        }
      }
    },
    {
      "Sid" : "BedrockAgentCoreS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::bedrock-agentcore-gateway-*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:CalledViaLast" : "bedrock-agentcore.amazonaws.com",
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BedrockAgentCoreGatewayLambdaAccess",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:*"
      ]
    },
    {
      "Sid" : "BedrockAgentCoreGatewayApiGateway",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis/*/stages/*/exports/*"
      ]
    },
    {
      "Sid" : "LoggingAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:Get*",
        "logs:List*",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:Describe*",
        "logs:TestMetricFilter",
        "logs:FilterLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/bedrock-agentcore/*",
        "arn:aws:logs:*:*:log-group:/aws/application-signals/data:*",
        "arn:aws:logs:*:*:log-group:aws/spans:*"
      ]
    },
```

```
    {
      "Sid" : "ObservabilityReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalingPolicies",
        "application-signals:BatchGet*",
        "application-signals:Get*",
        "application-signals:List*",
        "autoscaling:Describe*",
        "cloudwatch:BatchGet*",
        "cloudwatch:Describe*",
        "cloudwatch:GenerateQuery",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "oam:ListSinks",
        "rum:BatchGet*",
        "rum:Get*",
        "rum:List*",
        "synthetics:Describe*",
        "synthetics:Get*",
        "synthetics:List*",
        "xray:BatchGet*",
        "xray:Get*",
        "xray:List*",
        "xray:StartTraceRetrieval",
        "xray:CancelTraceRetrieval",
        "logs:DescribeLogGroups",
        "logs:StartLiveTail",
        "logs:StopLiveTail"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TransactionSearchXRayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "xray:GetTraceSegmentDestination",
        "xray:UpdateTraceSegmentDestination",
        "xray:GetIndexingRules",
        "xray:UpdateIndexingRule"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "TransactionSearchLogGroupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/application-signals/data:*",
        "arn:aws:logs:*:*:log-group:aws/spans:*"
      ]
    },
    {
      "Sid" : "TransactionSearchLogsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeResourcePolicies",
        "logs:PutResourcePolicy"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TransactionSearchApplicationSignalsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "application-signals:StartDiscovery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsCreateServiceLinkedRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/application-
signals.cloudwatch.amazonaws.com/AWSServiceRoleForCloudWatchApplicationSignals",
      "Condition" : {
        "StringLike" : {
```

```
          "iam:AWSServiceName" : "application-signals.cloudwatch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchApplicationSignalsGetRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/application-
signals.cloudwatch.amazonaws.com/AWSServiceRoleForCloudWatchApplicationSignals"
    },
    {
      "Sid" : "CreateBedrockAgentCoreNetworkServiceLinkedRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/network.bedrock-
agentcore.amazonaws.com/AWSServiceRoleForBedrockAgentCoreNetwork",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "network.bedrock-agentcore.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CreateBedrockAgentCoreRuntimeIdentityServiceLinkedRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/runtime-identity.bedrock-
agentcore.amazonaws.com/AWSServiceRoleForBedrockAgentCoreRuntimeIdentity",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "runtime-identity.bedrock-agentcore.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchApplicationSignalsCloudTrailPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateServiceLinkedChannel"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:channel/aws-service-channel/application-
signals/*"
    },
```

```
    {
      "Sid" : "BedrockAgentCoreRuntimeS3WriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutBucketPolicy",
        "s3:PutBucketVersioning",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::bedrock-agentcore-runtime-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BedrockAgentCoreRuntimeS3ReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket",
        "s3:ListBucketVersions"
      ],
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringEquals" : {
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BedrockAgentCoreRuntimeS3ListAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Sid" : "BedrockAgentCoreRuntimeECRAccess",
      "Effect" : "Allow",
      "Action" : [
        "ecr:DescribeRepositories",
        "ecr:DescribeImages",
        "ecr:ListImages"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/*"
      ]
    },
    {
      "Sid" : "AgentCoreEvaluationCloudWatchLogCreate",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/bedrock-agentcore/evaluations/*"
      ]
    },
    {
      "Sid" : "AgentCoreEvaluationCloudWatchLogIndexAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:PutIndexPolicy",
        "logs:DescribeIndexPolicies"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:aws/spans",
        "arn:aws:logs:*:*:log-group:aws/spans:*"
      ]
    },
    {
      "Sid" : "AgentCoreEvaluationBedrockInvokeAccess",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
```

```
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*",
        "arn:aws:bedrock:*:*:inference-profile/*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

BedrockAgentCoreNetworkServiceRolePolicy

説明: VPC モードで Amazon Bedrock AgentCore を実行するために必要な他の AWS サービスリソースへのアクセスを許可します

`BedrockAgentCoreNetworkServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2025 年 9 月 19 日 22:04 UTC
- 編集日時: 2025 年 9 月 19 日 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/BedrockAgentCoreNetworkServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCreateEniInAnySubnet",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:subnet/*"
    },
    {
      "Sid" : "AllowCreateEniWithSecurityGroups",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:security-group/*"
    },
    {
      "Sid" : "AllowCreateEniWithBedrockManagedRequestTag",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonBedrockAgentCoreManaged"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/AmazonBedrockAgentCoreManaged" : "true"
        }
      }
    },
    {
      "Sid" : "AllowTagEniOnCreate",
```

```
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        }
      }
    },
    {
      "Sid" : "AllowManageEniWhenBedrockManaged",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface",
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses",
        "ec2:CreateNetworkInterfacePermission"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonBedrockAgentCoreManaged" : "true"
        }
      }
    },
    {
      "Sid" : "AllowGetSecurityGroupsForVpc",
      "Effect" : "Allow",
      "Action" : [
        "ec2:GetSecurityGroupsForVPC"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Sid" : "AllowDescribeNetworkingResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

BedrockAgentCoreRuntimeIdentityServiceRolePolicy

説明: Amazon Bedrock AgentCore ランタイムの認証と認可に必要な ID およびトークン管理リソースへのアクセスを許可します。

BedrockAgentCoreRuntimeIdentityServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2025 年 10 月 11 日 01:04 UTC
- 編集日時: 2025 年 10 月 11 日 01:04 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/BedrockAgentCoreRuntimeIdentityServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Sid" : "AllowWorkloadIdentityAccess",
    "Effect" : "Allow",
    "Action" : [
      "bedrock-agentcore:GetWorkloadAccessToken",
      "bedrock-agentcore:GetWorkloadAccessTokenForJWT",
      "bedrock-agentcore:GetWorkloadAccessTokenForUserId"
    ],
    "Resource" : [
      "arn:aws:bedrock-agentcore:*:*:workload-identity-directory/default",
      "arn:aws:bedrock-agentcore:*:*:workload-identity-directory/default/workload-
identity/*"
    ]
  }
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

Billing

説明: 請求とコスト管理の権限を付与します。これには、アカウントの使用状況の閲覧、ならびに予算および支払い方法の修正および閲覧が含まれます。

`Billing` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `Billing` をアタッチできます。

ポリシーの詳細

- タイプ: ジョブ機能ポリシー
- 作成日時: 2016 年 11 月 10 日 17:33 UTC

- 編集日時: 2025 年 11 月 18 日 21:49 UTC
- ARN: arn:aws:iam::aws:policy/job-function/Billing

ポリシーのバージョン

ポリシーのバージョン: v17 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
        "aws-portal:*Billing",
        "aws-portal:*PaymentMethods",
        "aws-portal:*Usage",
        "billing:CreateBillingView",
        "billing:DeleteBillingView",
        "billing:GetBillingData",
        "billing:GetBillingDetails",
        "billing:GetBillingNotifications",
        "billing:GetBillingPreferences",
        "billing:GetBillingView",
        "billing:GetContractInformation",
        "billing:GetCredits",
        "billing:GetIAMAccessPreference",
        "billing:GetSellerOfRecord",
        "billing:ListBillingViews",
        "billing:PutContractInformation",
        "billing:RedeemCredits",
        "billing:GetResourcePolicy",
        "billing:ListSourceViewsForBillingView",
        "billing:ListTagsForResource",
        "billing:TagResource",
```

```
            "billing:UntagResource",
            "billing:UpdateBillingPreferences",
            "billing:UpdateBillingView",
            "billing:UpdateIAMAccessPreference",
            "budgets:CreateBudgetAction",
            "budgets:DeleteBudgetAction",
            "budgets:DescribeBudgetActionsForBudget",
            "budgets:DescribeBudgetAction",
            "budgets:DescribeBudgetActionsForAccount",
            "budgets:DescribeBudgetActionHistories",
            "budgets:ExecuteBudgetAction",
            "budgets:ModifyBudget",
            "budgets:UpdateBudgetAction",
            "budgets:ViewBudget",
            "ce:CreateCostCategoryDefinition",
            "ce:CreateNotificationSubscription",
            "ce:CreateReport",
            "ce:DeleteCostCategoryDefinition",
            "ce:DeleteNotificationSubscription",
            "ce:DeleteReport",
            "ce:DescribeCostCategoryDefinition",
            "ce:GetCostAndUsage",
            "ce:ListCostAllocationTags",
            "ce:ListCostCategoryDefinitions",
            "ce:ListTagsForResource",
            "ce:TagResource",
            "ce:UpdateCostAllocationTagsStatus",
            "ce:UpdateNotificationSubscription",
            "ce:UpdatePreferences",
            "ce:UpdateReport",
            "ce:UpdateCostCategoryDefinition",
            "ce:UntagResource",
            "ce:StartCostAllocationTagBackfill",
            "ce:ListCostAllocationTagBackfillHistory",
            "ce:GetTags",
            "ce:GetDimensionValues",
            "consolidatedbilling:GetAccountBillingRole",
            "consolidatedbilling:ListLinkedAccounts",
            "cur:DeleteReportDefinition",
            "cur:DescribeReportDefinitions",
            "cur:GetClassicReport",
            "cur:GetClassicReportPreferences",
            "cur:GetUsageReport",
            "cur:ModifyReportDefinition",
```

```
        "cur:PutClassicReportPreferences",
        "cur:PutReportDefinition",
        "cur:ValidateReportDestination",
        "freetier:GetFreeTierAlertPreference",
        "freetier:GetFreeTierUsage",
        "freetier:PutFreeTierAlertPreference",
        "invoicing:BatchGetInvoiceProfile",
        "invoicing:CreateInvoiceUnit",
        "invoicing:DeleteInvoiceUnit",
        "invoicing:GetInvoiceEmailDeliveryPreferences",
        "invoicing:GetInvoicePDF",
        "invoicing:GetInvoiceUnit",
        "invoicing:GetInvoiceCorrection",
        "invoicing:ListInvoiceSummaries",
        "invoicing:ListInvoiceUnits",
        "invoicing:CreateProcurementPortalPreference",
        "invoicing:GetProcurementPortalPreference",
        "invoicing:PutProcurementPortalPreference",
        "invoicing:UpdateProcurementPortalPreferenceStatus",
        "invoicing:ListProcurementPortalPreferences",
        "invoicing:DeleteProcurementPortalPreference",
        "invoicing:ListTagsForResource",
        "invoicing:ListInvoiceCorrections",
        "invoicing:StartInvoiceCorrection",
        "invoicing:PutInvoiceEmailDeliveryPreferences",
        "invoicing:TagResource",
        "invoicing:UntagResource",
        "invoicing:UpdateInvoiceUnit",
        "mapcredits:ListQuarterSpend",
        "mapcredits:ListAssociatedPrograms",
        "mapcredits:ListQuarterCredits",
        "payments:CreateFinancingApplication",
        "payments:CreatePaymentInstrument",
        "payments:DeletePaymentInstrument",
        "payments:GetFinancingApplication",
        "payments:GetFinancingLine",
        "payments:GetFinancingLineWithdrawal",
        "payments:GetFinancingOption",
        "payments:GetPaymentInstrument",
        "payments:GetPaymentStatus",
        "payments:ListFinancingApplications",
        "payments:ListFinancingLines",
        "payments:ListFinancingLineWithdrawals",
        "payments:ListPaymentPreferences",
```

```
        "payments:ListPaymentProgramOptions",
        "payments:ListPaymentProgramStatus",
        "payments:ListTagsForResource",
        "payments:ListPaymentInstruments",
        "payments:MakePayment",
        "payments:TagResource",
        "payments:UntagResource",
        "payments:UpdateFinancingApplication",
        "payments:UpdatePaymentInstrument",
        "payments:UpdatePaymentPreferences",
        "pricing:DescribeServices",
        "purchase-orders:AddPurchaseOrder",
        "purchase-orders:DeletePurchaseOrder",
        "purchase-orders:GetPurchaseOrder",
        "purchase-orders:ListPurchaseOrderInvoices",
        "purchase-orders:ListPurchaseOrders",
        "purchase-orders:ListTagsForResource",
        "purchase-orders:ModifyPurchaseOrders",
        "purchase-orders:TagResource",
        "purchase-orders:UntagResource",
        "purchase-orders:UpdatePurchaseOrder",
        "purchase-orders:UpdatePurchaseOrderStatus",
        "purchase-orders:ViewPurchaseOrders",
        "support:CreateCase",
        "support:AddAttachmentsToSet",
        "sustainability:GetCarbonFootprintSummary",
        "tax:BatchPutTaxRegistration",
        "tax:DeleteTaxRegistration",
        "tax:GetExemptions",
        "tax:GetTaxInheritance",
        "tax:GetTaxInterview",
        "tax:GetTaxRegistration",
        "tax:GetTaxRegistrationDocument",
        "tax:ListTaxRegistrations",
        "tax:PutTaxInheritance",
        "tax:PutTaxInterview",
        "tax:PutTaxRegistration",
        "tax:UpdateExemptions"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

BudgetsServiceRolePolicy

説明: Budgets がアカウント境界を越えて共有されている請求ビューへのアクセスを検証できるようにします。

`BudgetsServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2025 年 7 月 30 日 21:07 UTC
- 編集日時: 2025 年 7 月 30 日 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/BudgetsServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "billing:GetBillingViewData"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

CertificateManagerServiceRolePolicy

説明: Amazon Certificate Manager サービスロールポリシー

`CertificateManagerServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 6 月 25 日 17:56 UTC
- 編集日時: 2020 年 6 月 25 日 17:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CertificateManagerServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate",
        "acm-pca:GetCertificate"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

ClientVPNServiceConnectionsRolePolicy

説明: AWS クライアント VPN がクライアント VPN エンドポイント接続を管理できるようにするポリシー。

`ClientVPNServiceConnectionsRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 8 月 12 日 19:48 UTC
- 編集日時: 2020 年 8 月 12 日 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ClientVPNServiceConnectionsRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:AWSClientVPN-*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

ClientVPNServiceRolePolicy

説明: AWS クライアント VPN がクライアント VPN エンドポイントを管理できるようにするポリシー。

`ClientVPNServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 12 月 10 日 21:20 UTC
- 編集日時: 2020 年 8 月 12 日 19:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ClientVPNServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

CloudFormationStackSetsOrgAdminServiceRolePolicy

説明: CloudFormation StackSets (組織マスターアカウント) 用サービスロール

`CloudFormationStackSetsOrgAdminServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 12 月 10 日 00:20 UTC
- 編集日時: 2019 年 12 月 10 日 00:20 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudFormationStackSetsOrgAdminServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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-*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

CloudFormationStackSetsOrgMemberServiceRolePolicy

説明: CloudFormation StackSets (組織メンバーアカウント) のサービスロール

`CloudFormationStackSetsOrgMemberServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 12 月 9 日 23:52 UTC
- 編集日時: 2019 年 12 月 9 日 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudFormationStackSetsOrgMemberServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

CloudFrontFullAccess

説明: CloudFront コンソールへのフルアクセスの他に、 AWS マネジメントコンソール経由で Amazon S3 バケットを一覧表示する機能を提供します。

`CloudFrontFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `CloudFrontFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:39 UTC
- 編集日時: 2025 年 11 月 18 日 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/CloudFrontFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v10 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "cfflistbuckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
```

```
      "Sid" : "cffullaccess",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "cloudfront:*",
        "cloudfront-keyvaluestore:*",
        "iam:ListServerCertificates",
        "waf:ListWebACLs",
        "waf:GetWebACL",
        "wafv2:ListWebACLs",
        "wafv2:GetWebACL",
        "wafv2:CreateWebACL",
        "kinesis:ListStreams",
        "ec2:DescribeInstances",
        "elasticloadbalancing:DescribeLoadBalancers",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeIpamPools",
        "ec2:GetIpamPoolCidrs",
        "pricingplanmanager:ListSubscriptions",
        "pricingplanmanager:CreateSubscription"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "cfrequestcertificate",
      "Effect" : "Allow",
      "Action" : [
        "acm:RequestCertificate"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "cloudfront.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "cffdescribestream",
      "Effect" : "Allow",
      "Action" : [
        "kinesis:DescribeStream"
      ],
      "Resource" : "arn:aws:kinesis:*:*:*"
```

```
    },
    {
      "Sid" : "cfflistroles",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "arn:aws:iam::*:*"
    },
    {
      "Sid" : "ppmFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "pricingplanmanager:AssociateResourcesToSubscription",
        "pricingplanmanager:CancelSubscription",
        "pricingplanmanager:CancelSubscriptionChange",
        "pricingplanmanager:DisassociateResourcesFromSubscription",
        "pricingplanmanager:GetSubscription",
        "pricingplanmanager:UpdateSubscription"
      ],
      "Resource" : "arn:aws:pricingplanmanager::*:subscription:*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

CloudFrontReadOnlyAccess

説明: 経由で CloudFront ディストリビューション設定情報とリストディストリビューションへのアクセスを提供します AWS マネジメントコンソール。

`CloudFrontReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに CloudFrontReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:39 UTC
- 編集日時: 2025 年 11 月 18 日 17:19 UTC
- ARN: arn:aws:iam::aws:policy/CloudFrontReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "cfReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "cloudfront:Describe*",
        "cloudfront:Get*",
        "cloudfront:List*",
        "cloudfront-keyvaluestore:Describe*",
        "cloudfront-keyvaluestore:Get*",
        "cloudfront-keyvaluestore:List*",
        "iam:ListServerCertificates",
        "route53:List*",
        "waf:ListWebACLs",
```

```
        "waf:GetWebACL",
        "wafv2:ListWebACLs",
        "wafv2:GetWebACL",
        "ec2:DescribeIpamPools",
        "ec2:GetIpamPoolCidrs",
        "pricingplanmanager:ListSubscriptions",
        "pricingplanmanager:GetSubscription"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

CloudHSMServiceRolePolicy

説明: CloudHSM が使用または管理する AWS リソースへのアクセスを有効にします

CloudHSMServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 11 月 6 日 19:12 UTC
- 編集日時: 2017 年 11 月 6 日 19:12 UTC

- ARN: arn:aws:iam::aws:policy/aws-service-role/CloudHSMServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

CloudSearchFullAccess

説明: Amazon CloudSearch 設定サービスへのフルアクセスを提供します。

CloudSearchFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに CloudSearchFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:39 UTC
- 編集日時: 2015 年 2 月 6 日 18:39 UTC
- ARN: arn:aws:iam::aws:policy/CloudSearchFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudsearch:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

CloudSearchReadOnlyAccess

説明: Amazon CloudSearch 設定サービスへの読み取り専用アクセスを提供します。

`CloudSearchReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `CloudSearchReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:39 UTC
- 編集日時: 2015 年 2 月 6 日 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/CloudSearchReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudsearch:Describe*",
        "cloudsearch:List*"
      ],
```

```
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

CloudTrailEventContext

説明: このサービスにリンクされたロールにより、CloudTrail はリソース所有者の CloudTrail イベントにリソースタグを取得して追加できます。

`CloudTrailEventContext` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2025 年 5 月 15 日 13:52 UTC
- 編集日時: 2025 年 5 月 15 日 13:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudTrailEventContext`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudTrailEventContextPermissionForTag",
      "Effect" : "Allow",
      "Action" : "tag:GetResources",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowEventBridgeRuleCreation",
      "Effect" : "Allow",
      "Action" : "events:PutRule",
      "Resource" : "arn:aws:events:*:*:rule/CloudTrailEventContext*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "events:source" : "aws.tag"
        },
        "StringEquals" : {
          "events:creatorAccount" : "${aws:PrincipalAccount}",
          "events:detail-type" : "Tag Change on Resource",
          "events:ManagedBy" : "context.cloudtrail.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowEventBridgeRuleWrite",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:DeleteRule",
        "events:RemoveTargets"
```

```
      ],
      "Resource" : "arn:aws:events:*:*:rule/CloudTrailEventContext*",
      "Condition" : {
        "StringEquals" : {
          "events:creatorAccount" : "${aws:PrincipalAccount}",
          "events:ManagedBy" : "context.cloudtrail.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowEventBridgeRuleRead",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Condition" : {
        "StringEquals" : {
          "events:creatorAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : "arn:aws:events:*:*:rule/CloudTrailEventContext*"
    },
    {
      "Sid" : "AllowEventBridgeRuleList",
      "Effect" : "Allow",
      "Action" : [
        "events:ListRules"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

CloudTrailServiceRolePolicy

説明: CloudTrail ServiceLinkedRole のアクセス許可ポリシー

`CloudTrailServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 10 月 24 日 21:21 UTC
- 編集日時: 2023 年 11 月 27 日 01:18 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudTrailServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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}"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

CloudWatch-CrossAccountAccess

説明: CloudWatch が現在のアカウントに代わってリモートアカウントの CloudWatch-CrossAccountSharing ロールを引き受け、クロスアカウントおよびクロスリージョンでデータを表示できるようにします

`CloudWatch-CrossAccountAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 7 月 23 日 09:59 UTC
- 編集日時: 2019 年 7 月 23 日 09:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatch-CrossAccountAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/CloudWatch-CrossAccountSharing*"
      ],
      "Effect" : "Allow"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

CloudWatchActionsEC2Access

説明: CloudWatch アラームおよびメトリクスと EC2 メタデータへの読み取り専用のアクセスを提供します。EC2 インスタンスを停止、終了、再起動するためのアクセスを提供します。

`CloudWatchActionsEC2Access` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `CloudWatchActionsEC2Access` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 7 月 7 日 00:00 UTC
- 編集日時: 2015 年 7 月 7 日 00:00 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchActionsEC2Access`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:Describe*",
        "ec2:Describe*",
        "ec2:RebootInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

CloudWatchAgentAdminPolicy

説明: AmazonCloudWatchAgent を使用するために必要なフルアクセス許可。

`CloudWatchAgentAdminPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `CloudWatchAgentAdminPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 3 月 7 日 00:52 UTC
- 編集日時: 2024 年 2 月 5 日 20:59 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchAgentAdminPolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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-*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

CloudWatchAgentServerPolicy

説明: サーバーで AmazonCloudWatchAgent を使用するために必要なアクセス許可

`CloudWatchAgentServerPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに CloudWatchAgentServerPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 3 月 7 日 01:06 UTC
- 編集日時: 2024 年 2 月 6 日 16:37 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchAgentServerPolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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-*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

CloudWatchApplicationInsightsFullAccess

説明: CloudWatch Application Insights および必要な依存関係へのフルアクセスを提供します。

`CloudWatchApplicationInsightsFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `CloudWatchApplicationInsightsFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 11 月 24 日 18:44 UTC

- 編集日時: 2022 年 1 月 25 日 17:51 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchApplicationInsightsFullAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

CloudWatchApplicationInsightsReadOnlyAccess

説明: CloudWatch Application Insights への読み取り専用アクセスを提供します。

`CloudWatchApplicationInsightsReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに CloudWatchApplicationInsightsReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 11 月 24 日 18:48 UTC
- 編集日時: 2020 年 11 月 24 日 18:48 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchApplicationInsightsReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "applicationinsights:Describe*",
        "applicationinsights:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する

- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

CloudwatchApplicationInsightsServiceLinkedRolePolicy

説明: Cloudwatch Application Insights 向けサービスリンクロールポリシー

`CloudwatchApplicationInsightsServiceLinkedRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 12 月 1 日 16:22 UTC
- 編集日時: 2024 年 7 月 25 日 16:24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudwatchApplicationInsightsServiceLinkedRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v25 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Sid" : "CloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:PutAnomalyDetector",
        "cloudwatch:DeleteAnomalyDetector",
        "cloudwatch:DescribeAnomalyDetectors"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CloudWatchLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:FilterLogEvents",
        "logs:GetLogEvents",
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EventBridge",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CloudFormation",
      "Effect" : "Allow",
```

```
      "Action" : [
        "cloudFormation:CreateStack",
        "cloudFormation:UpdateStack",
        "cloudFormation:DeleteStack",
        "cloudFormation:DescribeStackResources",
        "cloudFormation:UpdateTerminationProtection"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/ApplicationInsights-*"
      ]
    },
    {
      "Sid" : "CloudFormationStacks",
      "Effect" : "Allow",
      "Action" : [
        "cloudFormation:DescribeStacks",
        "cloudFormation:ListStackResources",
        "cloudFormation:ListStacks"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "Tag",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ResourceGroups",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:ListGroupResources",
        "resource-groups:GetGroupQuery",
        "resource-groups:GetGroup"
      ],
      "Resource" : [
        "*"
      ]
```

```
    },
    {
      "Sid" : "ApplicationInsightsResourceGroup",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:DeleteGroup"
      ],
      "Resource" : [
        "arn:aws:resource-groups:*:*:group/ApplicationInsights-*"
      ]
    },
    {
      "Sid" : "ElasticLoadBalancing",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AutoScaling",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAutoScalingGroups"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SSMParameter",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter",
        "ssm:DeleteParameter",
        "ssm:AddTagsToResource",
        "ssm:RemoveTagsFromResource",
        "ssm:GetParameters"
      ],
```

```
      "Resource" : "arn:aws:ssm:*:*:parameter/AmazonCloudWatch-ApplicationInsights-*"
    },
    {
      "Sid" : "SSMAssociation",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:UpdateAssociation",
        "ssm:DeleteAssociation",
        "ssm:DescribeAssociation"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:association/*",
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*:*:document/AWSEC2-
ApplicationInsightsCloudwatchAgentInstallAndConfigure",
        "arn:aws:ssm:*:*:document/AWS-ConfigureAWSPackage",
        "arn:aws:ssm:*:*:document/AmazonCloudWatch-ManageAgent"
      ]
    },
    {
      "Sid" : "SSMOpsItem",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetOpsItem",
        "ssm:CreateOpsItem",
        "ssm:DescribeOpsItems",
        "ssm:UpdateOpsItem",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SSMTags",
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:opsitem/*"
    },
    {
```

```
      "Sid" : "SSMGetCommandInvocation",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListCommandInvocations",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SSMSendCommand",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:document/AWSEC2-CheckPerformanceCounterSets",
        "arn:aws:ssm:*:*:document/AWS-ConfigureAWSPackage",
        "arn:aws:ssm:*:*:document/AWSEC2-DetectWorkload",
        "arn:aws:ssm:*:*:document/AmazonCloudWatch-ManageAgent"
      ]
    },
    {
      "Sid" : "EC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumeStatus",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeNatGateways"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "RDS",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters"
      ],
```

```
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "Lambda",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions",
        "lambda:GetFunctionConfiguration",
        "lambda:ListEventSourceMappings"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EventBridgeManagedRule",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets",
        "events:DeleteRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/AmazonCloudWatch-ApplicationInsights-*"
      ]
    },
    {
      "Sid" : "XRay",
      "Effect" : "Allow",
      "Action" : [
        "xray:GetServiceGraph",
        "xray:GetTraceSummaries",
        "xray:GetTimeSeriesServiceStatistics",
        "xray:GetTraceGraph"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DynamoDB",
```

```
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListTables",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeContributorInsights",
        "dynamodb:DescribeTimeToLive"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ApplicationAutoscaling",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "S3",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:GetMetricsConfiguration",
        "s3:GetReplicationConfiguration"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "States",
      "Effect" : "Allow",
      "Action" : [
        "states:ListStateMachines",
        "states:DescribeExecution",
        "states:DescribeStateMachine",
        "states:GetExecutionHistory"
      ],
      "Resource" : [
        "*"
```

```
      ]
    },
    {
      "Sid" : "APIGateway",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ECS",
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeClusters",
        "ecs:DescribeContainerInstances",
        "ecs:DescribeServices",
        "ecs:DescribeTaskDefinition",
        "ecs:DescribeTasks",
        "ecs:DescribeTaskSets",
        "ecs:ListClusters",
        "ecs:ListContainerInstances",
        "ecs:ListServices",
        "ecs:ListTasks"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ECSCluster",
      "Effect" : "Allow",
      "Action" : [
        "ecs:UpdateClusterSettings"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:cluster/*"
      ]
    },
    {
      "Sid" : "EKS",
      "Effect" : "Allow",
```

```
      "Action" : [
        "eks:DescribeCluster",
        "eks:DescribeFargateProfile",
        "eks:DescribeNodegroup",
        "eks:ListClusters",
        "eks:ListFargateProfiles",
        "eks:ListNodegroups",
        "fsx:DescribeFileSystems",
        "fsx:DescribeVolumes"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SNS",
      "Effect" : "Allow",
      "Action" : [
        "sns:GetSubscriptionAttributes",
        "sns:GetTopicAttributes",
        "sns:GetSMSAttributes",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SQS",
      "Effect" : "Allow",
      "Action" : [
        "sqs:ListQueues"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchLogsDeleteSubscriptionFilter",
      "Effect" : "Allow",
      "Action" : [
        "logs:DeleteSubscriptionFilter"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:*"
```

```
      ]
    },
    {
      "Sid" : "CloudWatchLogsCreateSubscriptionFilter",
      "Effect" : "Allow",
      "Action" : [
        "logs:PutSubscriptionFilter"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:*",
        "arn:aws:logs:*:*:destination:AmazonCloudWatch-ApplicationInsights-
LogIngestionDestination*"
      ]
    },
    {
      "Sid" : "EFS",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeFileSystems"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "Route53",
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
        "route53:GetHealthCheck",
        "route53:ListHostedZones",
        "route53:ListHealthChecks",
        "route53:ListQueryLoggingConfigs"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "Route53Resolver",
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:ListFirewallRuleGroupAssociations",
        "route53resolver:GetFirewallRuleGroup",
```

```
        "route53resolver:ListFirewallRuleGroups",
        "route53resolver:ListResolverEndpoints",
        "route53resolver:GetResolverQueryLogConfig",
        "route53resolver:ListResolverQueryLogConfigs",
        "route53resolver:ListResolverQueryLogConfigAssociations",
        "route53resolver:GetResolverEndpoint",
        "route53resolver:GetFirewallRuleGroupAssociation"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

CloudWatchApplicationSignalsFullAccess

説明: CloudWatch Application Signals サービスへのフルアクセスと、サービスの使用と運用に必要な依存関係へのスコープ付きアクセスを提供します。

`CloudWatchApplicationSignalsFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `CloudWatchApplicationSignalsFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 6 月 6 日 22:50 UTC
- 編集日時: 2025 年 11 月 20 日 19:34 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchApplicationSignalsFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchApplicationSignalsFullAccessPermissions",
      "Effect" : "Allow",
      "Action" : "application-signals:*",
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsAlarmsPermissions",
      "Effect" : "Allow",
      "Action" : "cloudwatch:DescribeAlarms",
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsMetricsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsLogsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:GetQueryResults",
        "logs:DescribeLogGroups"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsSyntheticsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "synthetics:DescribeCanaries",
        "synthetics:DescribeCanariesLastRun",
        "synthetics:GetCanaryRuns"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsRumPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rum:BatchCreateRumMetricDefinitions",
        "rum:BatchDeleteRumMetricDefinitions",
        "rum:BatchGetRumMetricDefinitions",
        "rum:GetAppMonitor",
        "rum:GetAppMonitorData",
        "rum:ListAppMonitors",
        "rum:PutRumMetricsDestination",
        "rum:UpdateRumMetricDefinition"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsXrayTracePermissions",
      "Effect" : "Allow",
      "Action" : [
        "xray:GetTraceSummaries"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsXrayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "xray:StartTraceRetrieval",
        "xray:ListRetrievedTraces",
        "xray:BatchGetTraces",
        "xray:GetTraceSegmentDestination"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "application-signals.cloudwatch.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CloudWatchApplicationSignalsPutMetricAlarmPermissions",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricAlarm",
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:SLO-AttainmentGoalAlarm-*",
        "arn:aws:cloudwatch:*:*:alarm:SLO-WarningAlarm-*",
        "arn:aws:cloudwatch:*:*:alarm:SLI-HealthAlarm-*"
      ]
    },
    {
      "Sid" : "CloudWatchApplicationSignalsCreateServiceLinkedRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/application-
signals.cloudwatch.amazonaws.com/AWSServiceRoleForCloudWatchApplicationSignals",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "application-signals.cloudwatch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchApplicationSignalsGetRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/application-
signals.cloudwatch.amazonaws.com/AWSServiceRoleForCloudWatchApplicationSignals"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsSnsWritePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:Subscribe"
```

```
      ],
      "Resource" : "arn:aws:sns:*:*:cloudwatch-application-signals-*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsSnsReadPermissions",
      "Effect" : "Allow",
      "Action" : "sns:ListTopics",
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsCloudTrailPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateServiceLinkedChannel",
        "cloudtrail:GetChannel"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:channel/aws-service-channel/application-
signals/*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsCloudTrailListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:ListChannels"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsServiceQuotaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : [
        "arn:aws:servicequotas:*:*:s3/*",
        "arn:aws:servicequotas:*:*:dynamodb/*",
        "arn:aws:servicequotas:*:*:kinesis/*",
        "arn:aws:servicequotas:*:*:sns/*",
        "arn:aws:servicequotas:*:*:bedrock/*",
        "arn:aws:servicequotas:*:*:lambda/*",
        "arn:aws:servicequotas:*:*:fargate/*",
        "arn:aws:servicequotas:*:*:elasticloadbalancing/*",
        "arn:aws:servicequotas:*:*:ec2/*"
      ]
```

```
    },
    {
      "Sid" : "CloudWatchApplicationSignalsResourceExplorerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:Search"
      ],
      "Resource" : [
        "arn:aws:resource-explorer-2:*::view/AWSServiceViewForApplicationSignals/
service-view",
        "arn:aws:resource-explorer-2:*::view/
AWSServiceViewForApplicationSignalsOrgScopeProd/service-view"
      ]
    },
    {
      "Sid" : "CloudWatchApplicationSignalsResourceExplorerSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/resource-
explorer-2.amazonaws.com/AWSServiceRoleForResourceExplorer",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "resource-explorer-2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CloudWatchApplicationSignalsResourceExplorerCreateIndexPermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:CreateIndex"
      ],
      "Resource" : "arn:aws:resource-explorer-2:*:*:index/*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsOAMAttachedLinksPermissions",
      "Effect" : "Allow",
      "Action" : [
        "oam:ListAttachedLinks"
```

```
      ],
      "Resource" : "arn:aws:oam:*:*:sink/*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsOAMListSinksPermissions",
      "Effect" : "Allow",
      "Action" : [
        "oam:ListSinks"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

CloudWatchApplicationSignalsReadOnlyAccess

説明: CloudWatch Application Signals サービスへの読み取り専用アクセスと、サービスの使用に必要な依存関係へのスコープ付きアクセスを提供します。

`CloudWatchApplicationSignalsReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `CloudWatchApplicationSignalsReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 6 月 6 日 22:48 UTC
- 編集日時: 2025 年 11 月 20 日 19:34 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchApplicationSignalsReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchApplicationSignalsReadOnlyAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "application-signals:BatchGetServiceLevelObjectiveBudgetReport",
        "application-signals:GetService",
        "application-signals:GetServiceLevelObjective",
        "application-signals:ListServiceLevelObjectives",
        "application-signals:ListServiceDependencies",
        "application-signals:ListServiceDependents",
        "application-signals:ListServiceOperations",
        "application-signals:ListServices",
        "application-signals:ListTagsForResource",
        "application-signals:ListServiceStates",
        "application-signals:ListAuditFindings",
        "application-signals:ListGroupingAttributeDefinitions",
        "application-signals:ListServiceLevelObjectiveExclusionWindows",
        "application-signals:ListEntityEvents"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsGetRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/application-
signals.cloudwatch.amazonaws.com/AWSServiceRoleForCloudWatchApplicationSignals"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsLogsPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:GetQueryResults",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsAlarmsReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsMetricsReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsSyntheticsReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "synthetics:DescribeCanaries",
        "synthetics:DescribeCanariesLastRun",
        "synthetics:GetCanaryRuns"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsRumReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rum:BatchGetRumMetricDefinitions",
        "rum:GetAppMonitor",
        "rum:GetAppMonitorData",
        "rum:ListAppMonitors"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsXrayTracePermissions",
      "Effect" : "Allow",
      "Action" : [
        "xray:GetTraceSummaries"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsXrayReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "xray:StartTraceRetrieval",
        "xray:ListRetrievedTraces",
        "xray:BatchGetTraces",
        "xray:GetTraceSegmentDestination"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "application-signals.cloudwatch.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CloudWatchApplicationSignalsCloudTrailPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:GetChannel"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:channel/aws-service-channel/application-
signals/*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsCloudTrailListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:ListChannels"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsServiceQuotaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : [
        "arn:aws:servicequotas:*:*:s3/*",
        "arn:aws:servicequotas:*:*:dynamodb/*",
        "arn:aws:servicequotas:*:*:kinesis/*",
        "arn:aws:servicequotas:*:*:sns/*",
        "arn:aws:servicequotas:*:*:bedrock/*",
        "arn:aws:servicequotas:*:*:lambda/*",
        "arn:aws:servicequotas:*:*:fargate/*",
        "arn:aws:servicequotas:*:*:elasticloadbalancing/*",
        "arn:aws:servicequotas:*:*:ec2/*"
      ]
    },
    {
      "Sid" : "CloudWatchApplicationSignalsResourceExplorerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:Search"
      ],
      "Resource" : [
        "arn:aws:resource-explorer-2:*::view/AWSServiceViewForApplicationSignals/
service-view",
        "arn:aws:resource-explorer-2:*::view/
AWSServiceViewForApplicationSignalsOrgScopeProd/service-view"
      ]
    },
    {
      "Sid" : "CloudWatchApplicationSignalsOAMAttachedLinksPermissions",
      "Effect" : "Allow",
      "Action" : [
        "oam:ListAttachedLinks"
      ],
      "Resource" : "arn:aws:oam:*:*:sink/*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsOAMListSinksPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "oam:ListSinks"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

CloudWatchApplicationSignalsServiceRolePolicy

説明: ポリシーは、CloudWatch Application Signals に、他の関連 AWS サービスからモニタリングおよびタグ付けデータを収集するアクセス許可を付与します。

`CloudWatchApplicationSignalsServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 11 月 9 日 18:09 UTC
- 編集日時: 2025 年 11 月 14 日 21:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchApplicationSignalsServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "XRayPermission",
      "Effect" : "Allow",
      "Action" : [
        "xray:GetServiceGraph"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CWLogsPermission",
      "Effect" : "Allow",
      "Action" : [
        "logs:StartQuery",
        "logs:GetQueryResults"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/appsignals/*:*",
        "arn:aws:logs:*:*:log-group:/aws/application-signals/data:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "CWListMetricsPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:ListMetrics"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CWGetMetricDataPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "TagsPermission",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ApplicationSignalsPermission",
```

```
      "Effect" : "Allow",
      "Action" : [
        "application-signals:ListServiceLevelObjectiveExclusionWindows",
        "application-signals:GetServiceLevelObjective"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EC2AutoScalingPermission",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAutoScalingGroups"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ResourceExplorerReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:Search"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CloudTrailServiceLinkedChannelCreationPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateServiceLinkedChannel"
```

```
      ],
      "Resource" : [
        "arn:aws:cloudtrail:*:*:channel/aws-service-channel/application-signals/*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

CloudWatchAutomaticDashboardsAccess

説明: Lambda 関数などのオブジェクトのコンテンツなど、CloudWatch 自動ダッシュボードの表示に使用される CloudWatch 以外の API へのアクセスを提供します

`CloudWatchAutomaticDashboardsAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `CloudWatchAutomaticDashboardsAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 7 月 23 日 10:01 UTC
- 編集日時: 2021 年 4 月 20 日 13:05 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchAutomaticDashboardsAccess`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

CloudWatchCrossAccountSharingConfiguration

説明: オブザーバビリティ Access Manager のリンクを管理し、CloudWatch リソースの共有を確立する機能を提供

`CloudWatchCrossAccountSharingConfiguration` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `CloudWatchCrossAccountSharingConfiguration` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2022 年 11 月 27 日 14:01 UTC
- 編集日時: 2022 年 11 月 27 日 14:01 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchCrossAccountSharingConfiguration`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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/*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

CloudWatchEventsBuiltInTargetExecutionAccess

説明: Amazon CloudWatch Events の組み込みターゲットが、お客様に代わって EC2 アクションを実行することを許可します。

`CloudWatchEventsBuiltInTargetExecutionAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `CloudWatchEventsBuiltInTargetExecutionAccess` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2016 年 1 月 14 日 18:35 UTC
- 編集日時: 2016 年 1 月 14 日 18:35 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/CloudWatchEventsBuiltInTargetExecutionAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchEventsBuiltInTargetExecutionAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:Describe*",
        "ec2:RebootInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:CreateSnapshot"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

CloudWatchEventsFullAccess

説明: Amazon CloudWatch Events へのフルアクセスを提供します。

`CloudWatchEventsFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `CloudWatchEventsFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2016 年 1 月 14 日 18:37 UTC
- 編集日時: 2025 年 1 月 22 日 02:07 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchEventsFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EventBridgeActions",
      "Effect" : "Allow",
      "Action" : [
        "events:*",
        "schemas:*",
        "scheduler:*",
        "pipes:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMCreateServiceLinkedRoleForApiDestinations",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
apidestinations.events.amazonaws.com/
AWSServiceRoleForAmazonEventBridgeApiDestinations",
      "Condition" : {
        "StringEquals" : {
```

```
          "iam:AWSServiceName" : "apidestinations.events.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMCreateServiceLinkedRoleForAmazonEventBridgeSchemas",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/schemas.amazonaws.com/
AWSServiceRoleForSchemas",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "schemas.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SecretsManagerAccessForApiDestinations",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:events!*"
    },
    {
      "Sid" : "IAMPassRoleForCloudWatchEvents",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/AWS_Events_Invoke_Targets"
    },
    {
      "Sid" : "IAMPassRoleAccessForScheduler",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "scheduler.amazonaws.com"
        }
      }
```

```
    },
    {
      "Sid" : "IAMPassRoleAccessForPipes",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "pipes.amazonaws.com"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

CloudWatchEventsInvocationAccess

説明: Amazon CloudWatch Events がアカウントの AWS Kinesis Streams のストリームにイベントを中継できるようにします。

`CloudWatchEventsInvocationAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `CloudWatchEventsInvocationAccess` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2016 年 1 月 14 日 18:36 UTC

- 編集日時: 2016 年 1 月 14 日 18:36 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/CloudWatchEventsInvocationAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchEventsInvocationAccess",
      "Effect" : "Allow",
      "Action" : [
        "kinesis:PutRecord"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

CloudWatchEventsReadOnlyAccess

説明: Amazon CloudWatch Events への読み取り専用アクセスを提供します。

CloudWatchEventsReadOnlyAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに CloudWatchEventsReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2016 年 1 月 14 日 18:27 UTC
- 編集日時: 2022 年 12 月 1 日 16:29 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchEventsReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

CloudWatchEventsServiceRolePolicy

説明: Allow AWS CloudWatch は、アラームとイベントを使用して設定されたユーザーに代わってアクションを実行します。

CloudWatchEventsServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 11 月 17 日 00:42 UTC
- 編集日時: 2017 年 11 月 17 日 00:42 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/CloudWatchEventsServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

CloudWatchFullAccess

説明: CloudWatch へのフルアクセスを提供します。

`CloudWatchFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `CloudWatchFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2022 年 11 月 27 日 13:23 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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/*"
    }
  ]
```

```
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

CloudWatchFullAccessV2

説明: CloudWatch へのフルアクセスを提供します。

`CloudWatchFullAccessV2` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `CloudWatchFullAccessV2` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 8 月 1 日 11:32 UTC
- 編集日時: 2025 年 12 月 2 日 16:49 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchFullAccessV2`

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchFullAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalingPolicies",
        "application-signals:*",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribePolicies",
        "cloudwatch:*",
        "logs:*",
        "sns:CreateTopic",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "sns:Subscribe",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "oam:ListSinks",
        "observabilityadmin:GetCentralizationRuleForOrganization",
        "observabilityadmin:ListCentralizationRulesForOrganization",
        "observabilityadmin:CreateCentralizationRuleForOrganization",
        "observabilityadmin:UpdateCentralizationRuleForOrganization",
        "observabilityadmin:DeleteCentralizationRuleForOrganization",
        "observabilityadmin:StartTelemetryEvaluation",
        "observabilityadmin:GetTelemetryEvaluationStatus",
        "observabilityadmin:ListResourceTelemetry",
        "observabilityadmin:StopTelemetryEvaluation",
        "observabilityadmin:StartTelemetryEvaluationForOrganization",
        "observabilityadmin:GetTelemetryEvaluationStatusForOrganization",
        "observabilityadmin:ListResourceTelemetryForOrganization",
        "observabilityadmin:StopTelemetryEvaluationForOrganization",
        "observabilityadmin:CreateTelemetryRule",
        "observabilityadmin:GetTelemetryRule",
        "observabilityadmin:ListTelemetryRules",
        "observabilityadmin:UpdateTelemetryRule",
        "observabilityadmin:DeleteTelemetryRule",
        "observabilityadmin:CreateTelemetryRuleForOrganization",
        "observabilityadmin:GetTelemetryRuleForOrganization",
        "observabilityadmin:ListTelemetryRulesForOrganization",
        "observabilityadmin:UpdateTelemetryRuleForOrganization",
        "observabilityadmin:DeleteTelemetryRuleForOrganization",
```

```
        "observabilityadmin:GetTelemetryEnrichmentStatus",
        "observabilityadmin:StartTelemetryEnrichment",
        "observabilityadmin:StopTelemetryEnrichment",
        "observabilityadmin:TagResource",
        "observabilityadmin:UntagResource",
        "observabilityadmin:ListTagsForResource",
        "observabilityadmin:CreateTelemetryPipeline",
        "observabilityadmin:GetTelemetryPipeline",
        "observabilityadmin:UpdateTelemetryPipeline",
        "observabilityadmin:DeleteTelemetryPipeline",
        "observabilityadmin:ListTelemetryPipelines",
        "observabilityadmin:TestTelemetryPipeline",
        "observabilityadmin:ValidateTelemetryPipelineConfiguration",
        "observabilityadmin:CreateS3TableIntegration",
        "observabilityadmin:GetS3TableIntegration",
        "observabilityadmin:ListS3TableIntegrations",
        "observabilityadmin:DeleteS3TableIntegration",
        "rum:*",
        "synthetics:*",
        "xray:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsServiceLinkedRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/application-
signals.cloudwatch.amazonaws.com/AWSServiceRoleForCloudWatchApplicationSignals",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "application-signals.cloudwatch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EventsServicePermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/events.amazonaws.com/
AWSServiceRoleForCloudWatchEvents*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "events.amazonaws.com"
```

```
        }
      }
    },
    {
      "Sid" : "OAMReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "oam:ListAttachedLinks"
      ],
      "Resource" : "arn:aws:oam:*:*:sink/*"
    },
    {
      "Sid" : "CloudWatchCloudTrailPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateServiceLinkedChannel",
        "cloudtrail:GetChannel"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:channel/aws-service-channel/application-
signals/*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsCloudTrailListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:ListChannels"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchServiceQuotaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : [
        "arn:aws:servicequotas:*:*:s3/*",
        "arn:aws:servicequotas:*:*:dynamodb/*",
        "arn:aws:servicequotas:*:*:kinesis/*",
        "arn:aws:servicequotas:*:*:sns/*",
        "arn:aws:servicequotas:*:*:bedrock/*",
        "arn:aws:servicequotas:*:*:lambda/*",
        "arn:aws:servicequotas:*:*:fargate/*",
        "arn:aws:servicequotas:*:*:elasticloadbalancing/*",
```

```
        "arn:aws:servicequotas:*:*:ec2/*"
      ]
    },
    {
      "Sid" : "CloudWatchResourceExplorerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:Search"
      ],
      "Resource" : [
        "arn:aws:resource-explorer-2:*::view/AWSServiceViewForApplicationSignals/
service-view",
        "arn:aws:resource-explorer-2:*::view/
AWSServiceViewForApplicationSignalsOrgScopeProd/service-view"
      ]
    },
    {
      "Sid" : "CloudWatchResourceExplorerSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/resource-
explorer-2.amazonaws.com/AWSServiceRoleForResourceExplorer",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "resource-explorer-2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CloudWatchResourceExplorerCreateIndexPermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:CreateIndex"
      ],
      "Resource" : "arn:aws:resource-explorer-2:*:*:index/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "logs.amazonaws.com"
        },
        "ArnLike" : {
          "iam:AssociatedResourceArn" :
 "arn:aws:observabilityadmin:*:*:s3tableintegration/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "logs.amazonaws.com",
            "telemetry-pipelines.observabilityadmin.amazonaws.com"
          ]
        },
        "ArnLike" : {
          "iam:AssociatedResourceArn" : "arn:aws:observabilityadmin:*:*:telemetry-
pipeline/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3tables:CreateTableBucket",
        "s3tables:PutTableBucketEncryption"
      ],
      "Resource" : "arn:aws:s3tables:*:*:bucket/aws-cloudwatch",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "observabilityadmin.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3tables:PutTableBucketPolicy"
      ],
      "Resource" : "arn:aws:s3tables:*:*:bucket/aws-cloudwatch"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

CloudWatchInternetMonitorFullAccess

説明: Amazon CloudWatch Internet Monitor を操作するためのアクションへのフルアクセスを提供します。また、Amazon CloudWatch 、Amazon EC2、Amazon CloudFront 、Amazon WorkSpaces 、Elastic Load Balancing などの、アプリケーショントラフィックに関する情報をモニタリングおよび保存するための Internet Monitor サービスに必要な他のサービスへのアクセスも提供します。

`CloudWatchInternetMonitorFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `CloudWatchInternetMonitorFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 10 月 22 日 21:02 UTC
- 編集日時: 2024 年 10 月 22 日 21:02 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchInternetMonitorFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "FullAccessActions",
      "Effect" : "Allow",
      "Action" : [
        "internetmonitor:CreateMonitor",
        "internetmonitor:DeleteMonitor",
        "internetmonitor:GetHealthEvent",
        "internetmonitor:GetInternetEvent",
        "internetmonitor:GetMonitor",
        "internetmonitor:GetQueryResults",
        "internetmonitor:GetQueryStatus",
        "internetmonitor:Link",
        "internetmonitor:ListHealthEvents",
        "internetmonitor:ListInternetEvents",
        "internetmonitor:ListMonitors",
        "internetmonitor:ListTagsForResource",
        "internetmonitor:StartQuery",
        "internetmonitor:StopQuery",
        "internetmonitor:TagResource",
        "internetmonitor:UntagResource",
        "internetmonitor:UpdateMonitor"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ServiceLinkedRoleActions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/internetmonitor.amazonaws.com/
AWSServiceRoleForInternetMonitor",
```

```
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "internetmonitor.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "RolePolicyActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/internetmonitor.amazonaws.com/
AWSServiceRoleForInternetMonitor",
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : "arn:aws:iam::aws:policy/aws-service-role/
CloudWatchInternetMonitorServiceRolePolicy"
        }
      }
    },
    {
      "Sid" : "ReadOnlyActions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudfront:GetDistribution",
        "cloudfront:ListDistributions",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:DescribeLoadBalancers",
        "logs:DescribeLogGroups",
        "logs:GetQueryResults",
        "logs:StartQuery",
        "logs:StopQuery",
        "workspaces:DescribeWorkspaceDirectories"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

CloudWatchInternetMonitorReadOnlyAccess

説明: Amazon CloudWatch Internet Monitor を操作するためのアクションへの読み取り専用アクセスを提供します。また、Amazon CloudWatch の他のサービスへのアクセスも提供します。これには、CloudWatch メトリクスに関する情報を取得し、アプリケーショントラフィックに関する情報をモニタリングおよび保存するために Internet Monitor サービスを使用するために必要なロググエリを管理するポリシーが含まれます。

`CloudWatchInternetMonitorReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `CloudWatchInternetMonitorReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 11 月 12 日 23:11 UTC
- 編集日時: 2024 年 11 月 12 日 23:11 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchInternetMonitorReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadOnlyActions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "internetmonitor:GetHealthEvent",
        "internetmonitor:GetInternetEvent",
        "internetmonitor:GetMonitor",
        "internetmonitor:GetQueryResults",
        "internetmonitor:GetQueryStatus",
        "internetmonitor:ListHealthEvents",
        "internetmonitor:ListInternetEvents",
        "internetmonitor:ListMonitors",
        "internetmonitor:ListTagsForResource",
        "internetmonitor:StartQuery",
        "internetmonitor:StopQuery",
        "logs:DescribeLogGroups",
        "logs:GetQueryResults",
        "logs:StartQuery",
        "logs:StopQuery"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

CloudWatchInternetMonitorServiceRolePolicy

説明: Internet Monitor がユーザーに代わって EC2、Workspaces、CloudFront リソース、およびその他の必要なサービスにアクセスできるようにします。

`CloudWatchInternetMonitorServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 11 月 27 日 17:46 UTC
- 編集日時: 2023 年 7 月 20 日 04:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchInternetMonitorServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

CloudWatchLambdaApplicationSignalsExecutionRolePolicy

説明: X-Ray および CloudWatch Application Signals ロググループへの書き込みアクセスを提供します。

CloudWatchLambdaApplicationSignalsExecutionRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに CloudWatchLambdaApplicationSignalsExecutionRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 10 月 16 日 19:09 UTC
- 編集日時: 2024 年 10 月 16 日 19:09 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchLambdaApplicationSignalsExecutionRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchApplicationSignalsXrayWritePermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "xray:PutTraceSegments"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CloudWatchApplicationSignalsLogGroupWritePermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/application-signals/data:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

CloudWatchLambdaInsightsExecutionRolePolicy

説明: Lambda Insights 拡張機能に必要なポリシー

`CloudWatchLambdaInsightsExecutionRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに CloudWatchLambdaInsightsExecutionRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 10 月 7 日 19:27 UTC
- 編集日時: 2020 年 10 月 7 日 19:27 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchLambdaInsightsExecutionRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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:*"
    }
  ]
```

```
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

CloudWatchLogsCrossAccountSharingConfiguration

説明: オブザーバビリティ Access Manager のリンクを管理し、CloudWatch のログリソースの共有を確立する機能を提供

`CloudWatchLogsCrossAccountSharingConfiguration` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `CloudWatchLogsCrossAccountSharingConfiguration` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 11 月 27 日 13:55 UTC
- 編集日時: 2022 年 11 月 27 日 13:55 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLogsCrossAccountSharingConfiguration`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

CloudWatchLogsFullAccess

説明: CloudWatch Logs へのフルアクセスを提供します

CloudWatchLogsFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに CloudWatchLogsFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2025 年 12 月 2 日 16:34 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchLogsFullAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchLogsFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:*",
        "cloudwatch:GenerateQuery",
```

```
        "cloudwatch:GenerateQueryResultsSummary",
        "observabilityadmin:GetS3TableIntegration",
        "observabilityadmin:ListS3TableIntegrations",
        "observabilityadmin:ListTelemetryPipelines"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

CloudWatchLogsReadOnlyAccess

説明: CloudWatch Logs への読み取り専用アクセスを提供します

`CloudWatchLogsReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `CloudWatchLogsReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2025 年 12 月 2 日 16:34 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLogsReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchLogsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:Describe*",
        "logs:Get*",
        "logs:List*",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:TestMetricFilter",
        "logs:FilterLogEvents",
        "logs:StartLiveTail",
        "logs:StopLiveTail",
        "cloudwatch:GenerateQuery",
        "cloudwatch:GenerateQueryResultsSummary",
        "observabilityadmin:ListS3TableIntegrations",
        "observabilityadmin:GetS3TableIntegration",
        "observabilityadmin:ListTelemetryPipelines"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

CloudWatchNetworkFlowMonitorAgentPublishPolicy

説明: このポリシーは、テレメトリレポート (メトリクス) を Network Flow Monitor エンドポイントに送信するために、Amazon EC2 および Amazon EKS インスタンスリソースにアタッチされた IAM ロールで使用できます。

`CloudWatchNetworkFlowMonitorAgentPublishPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `CloudWatchNetworkFlowMonitorAgentPublishPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 12 月 1 日 22:51 UTC
- 編集日時: 2024 年 12 月 1 日 22:51 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchNetworkFlowMonitorAgentPublishPolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "networkflowmonitor:Publish"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

CloudWatchNetworkFlowMonitorServiceRolePolicy

説明: CloudWatchNetworkFlowMonitorServiceRolePolicy を IAM エンティティにアタッチすることはできません。このポリシーは、AWSServiceRoleForNetworkFlowMonitor という名前のサービスリンクロールにアタッチされます。このロールは、Network Flow Monitor エージェントによって収集されたネットワークテレメトリの集約結果を CloudWatch に発行します。また、サービスが AWS Organizations を使用してマルチアカウントシナリオの情報を取得することもできます。

`CloudWatchNetworkFlowMonitorServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2024 年 12 月 1 日 22:36 UTC
- 編集日時: 2025 年 4 月 29 日 10:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchNetworkFlowMonitorServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/NetworkFlowMonitor"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListAccounts",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount"
      ],
      "Resource" : [
        "arn:aws:organizations::*:account/*"
      ]
```

```
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

CloudWatchNetworkFlowMonitorTopologyServiceRolePolicy

説明: CloudWatchNetworkFlowMonitorTopologyServiceRolePolicy を IAM エンティティにアタッチすることはできません。このポリシーは、サービスにリンクされた AWSServiceRoleForNetworkFlowMonitor_Topology という名前のロールにアタッチされ、アカウントで Network Flow Monitor が使用するリソースのトポロジスナップショットを生成します。

`CloudWatchNetworkFlowMonitorTopologyServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2024 年 12 月 1 日 22:51 UTC
- 編集日時: 2025 年 12 月 10 日 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchNetworkFlowMonitorTopologyServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeCustomerGateways",
        "ec2:GetTransitGatewayRouteTableAssociations",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:SearchTransitGatewayRoutes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PrefixListStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeManagedPrefixLists",
        "ec2:GetManagedPrefixListEntries"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VPCEndpointStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServiceConfigurations"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

CloudWatchNetworkMonitorServiceRolePolicy

説明: CloudWatch Network Monitor が、EC2 および VPC リソースにアクセスして管理し、データの CloudWatch への公開、およびユーザーに代わって他の必要なサービスにアクセスできるようにします。

`CloudWatchNetworkMonitorServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 12 月 21 日 18:53 UTC
- 編集日時: 2025 年 12 月 12 日 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchNetworkMonitorServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PublishCw",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/NetworkMonitor"
        }
      }
    },
    {
      "Sid" : "DescribeAny",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:SearchTransitGatewayRoutes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DeleteModifyEc2Resources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface",
```

```
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/ManagedByCloudWatchNetworkMonitor" : "true"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

CloudWatchOpenSearchDashboardAccess

説明: このポリシーは、CloudWatch Logs コンソールで OpenSearch ダッシュボードを表示するためのユーザーアクセスを提供します。

`CloudWatchOpenSearchDashboardAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `CloudWatchOpenSearchDashboardAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 12 月 1 日 21:06 UTC
- 編集日時: 2024 年 12 月 1 日 21:06 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchOpenSearchDashboardAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchOpenSearchDashboardsIntegration",
      "Effect" : "Allow",
      "Action" : [
        "logs:ListIntegrations",
        "logs:GetIntegration",
        "logs:DescribeLogGroups",
        "opensearch:ApplicationAccessAll",
        "iam:ListRoles",
        "iam:ListUsers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchLogsOpensearchReadAPIs",
      "Effect" : "Allow",
      "Action" : [
        "aoss:BatchGetCollection",
        "aoss:BatchGetLifecyclePolicy",
        "es:ListApplications"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsAPIAccessAll",
```

```
      "Effect" : "Allow",
      "Action" : [
        "aoss:APIAccessAll"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aoss:collection" : "cloudwatch-logs-*"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsDQSCollectionPolicyAccess",
      "Effect" : "Allow",
      "Action" : [
        "aoss:GetAccessPolicy",
        "aoss:GetSecurityPolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com",
          "aoss:collection" : "cloudwatch-logs-*"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsApplicationResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "es:GetApplication"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com",
          "aws:ResourceTag/OpenSearchIntegration" : [
            "Dashboards"
          ]
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsDQSResourceQueryAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "es:GetDirectQueryDataSource"
      ],
      "Resource" : "arn:aws:opensearch:*:*:datasource/cloudwatch_logs_*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com",
          "aws:ResourceTag/CloudWatchOpenSearchIntegration" : [
            "Dashboards"
          ]
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsDirectQueryStatusAccess",
      "Effect" : "Allow",
      "Action" : [
        "opensearch:GetDirectQuery"
      ],
      "Resource" : "arn:aws:opensearch:*:*:datasource/cloudwatch_logs_*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

CloudWatchOpenSearchDashboardsFullAccess

説明: このポリシーは、CloudWatch Logs コンソールでダッシュボードを作成、更新、削除、または表示するための OpenSearch との統合を作成するためのユーザーアクセスを提供します。

`CloudWatchOpenSearchDashboardsFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに CloudWatchOpenSearchDashboardsFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 12 月 1 日 21:06 UTC
- 編集日時: 2024 年 12 月 1 日 21:06 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchOpenSearchDashboardsFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchOpenSearchDashboardsIntegration",
      "Effect" : "Allow",
      "Action" : [
        "logs:ListIntegrations",
        "logs:GetIntegration",
        "logs:DeleteIntegration",
        "logs:PutIntegration",
        "logs:DescribeLogGroups",
        "opensearch:ApplicationAccessAll",
        "iam:ListRoles",
        "iam:ListUsers"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "CloudWatchLogsOpensearchReadAPIs",
      "Effect" : "Allow",
      "Action" : [
        "aoss:BatchGetCollection",
        "aoss:BatchGetLifecyclePolicy",
        "es:ListApplications"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsOpensearchCreateServiceLinkedAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
opensearchservice.amazonaws.com/AWSServiceRoleForAmazonOpenSearchService",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "opensearchservice.amazonaws.com",
          "aws:CalledViaFirst" : "logs.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsObservabilityCreateServiceLinkedAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
observability.aoss.amazonaws.com/AWSServiceRoleForAmazonOpenSearchServerless",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "observability.aoss.amazonaws.com",
          "aws:CalledViaFirst" : "logs.amazonaws.com"
        }
      }
```

```
    },
    {
      "Sid" : "CloudWatchLogsCollectionRequestAccess",
      "Effect" : "Allow",
      "Action" : [
        "aoss:CreateCollection"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com",
          "aws:RequestTag/CloudWatchOpenSearchIntegration" : [
            "Dashboards"
          ]
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "CloudWatchOpenSearchIntegration"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsApplicationRequestAccess",
      "Effect" : "Allow",
      "Action" : [
        "es:CreateApplication"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com",
          "aws:RequestTag/OpenSearchIntegration" : [
            "Dashboards"
          ]
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "OpenSearchIntegration"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsCollectionResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "aoss:DeleteCollection"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com",
          "aws:ResourceTag/CloudWatchOpenSearchIntegration" : [
            "Dashboards"
          ]
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsApplicationResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "es:UpdateApplication",
        "es:GetApplication"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com",
          "aws:ResourceTag/OpenSearchIntegration" : [
            "Dashboards"
          ]
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsCollectionPolicyAccess",
      "Effect" : "Allow",
      "Action" : [
        "aoss:CreateSecurityPolicy",
        "aoss:CreateAccessPolicy",
        "aoss:DeleteAccessPolicy",
        "aoss:DeleteSecurityPolicy",
        "aoss:GetAccessPolicy",
        "aoss:GetSecurityPolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aoss:collection" : "cloudwatch-logs-*",
          "aws:CalledViaFirst" : "logs.amazonaws.com"
```

```
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsAPIAccessAll",
      "Effect" : "Allow",
      "Action" : [
        "aoss:APIAccessAll"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aoss:collection" : "cloudwatch-logs-*"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsIndexPolicyAccess",
      "Effect" : "Allow",
      "Action" : [
        "aoss:CreateAccessPolicy",
        "aoss:DeleteAccessPolicy",
        "aoss:GetAccessPolicy",
        "aoss:CreateLifecyclePolicy",
        "aoss:DeleteLifecyclePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aoss:index" : "cloudwatch-logs-*",
          "aws:CalledViaFirst" : "logs.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsDQSRequestQueryAccess",
      "Effect" : "Allow",
      "Action" : [
        "es:AddDirectQueryDataSource"
      ],
      "Resource" : "arn:aws:opensearch:*:*:datasource/cloudwatch_logs_*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com",
```

```
          "aws:RequestTag/CloudWatchOpenSearchIntegration" : [
            "Dashboards"
          ]
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "CloudWatchOpenSearchIntegration"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsStartDirectQueryAccess",
      "Effect" : "Allow",
      "Action" : [
        "opensearch:StartDirectQuery",
        "opensearch:GetDirectQuery"
      ],
      "Resource" : "arn:aws:opensearch:*:*:datasource/cloudwatch_logs_*"
    },
    {
      "Sid" : "CloudWatchLogsDQSResourceQueryAccess",
      "Effect" : "Allow",
      "Action" : [
        "es:GetDirectQueryDataSource",
        "es:DeleteDirectQueryDataSource"
      ],
      "Resource" : "arn:aws:opensearch:*:*:datasource/cloudwatch_logs_*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com",
          "aws:ResourceTag/CloudWatchOpenSearchIntegration" : [
            "Dashboards"
          ]
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsPassRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
```

```
          "iam:PassedToService" : "directquery.opensearchservice.amazonaws.com",
          "aws:CalledViaFirst" : "logs.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsAossTagsAccess",
      "Effect" : "Allow",
      "Action" : [
        "aoss:TagResource"
      ],
      "Resource" : "arn:aws:aoss:*:*:collection/*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com",
          "aws:ResourceTag/CloudWatchOpenSearchIntegration" : [
            "Dashboards"
          ]
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "CloudWatchOpenSearchIntegration"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsEsApplicationTagsAccess",
      "Effect" : "Allow",
      "Action" : [
        "es:AddTags"
      ],
      "Resource" : "arn:aws:opensearch:*:*:application/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/OpenSearchIntegration" : [
            "Dashboards"
          ],
          "aws:CalledViaFirst" : "logs.amazonaws.com"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "OpenSearchIntegration"
        }
      }
    },
    {
```

```
      "Sid" : "CloudWatchLogsEsDataSourceTagsAccess",
      "Effect" : "Allow",
      "Action" : [
        "es:AddTags"
      ],
      "Resource" : "arn:aws:opensearch:*:*:datasource/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CloudWatchOpenSearchIntegration" : [
            "Dashboards"
          ],
          "aws:CalledViaFirst" : "logs.amazonaws.com"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "CloudWatchOpenSearchIntegration"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

CloudWatchReadOnlyAccess

説明: CloudWatch への読み取り専用アクセスを提供します。

`CloudWatchReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `CloudWatchReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2025 年 12 月 2 日 16:49 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v14 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchReadOnlyAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalingPolicies",
        "application-signals:BatchGet*",
        "application-signals:Get*",
        "application-signals:List*",
        "autoscaling:Describe*",
        "cloudtrail:ListChannels",
        "cloudwatch:BatchGet*",
        "cloudwatch:Describe*",
        "cloudwatch:GenerateQuery",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "logs:Get*",
        "logs:List*",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:Describe*",
```

```
        "logs:TestMetricFilter",
        "logs:FilterLogEvents",
        "logs:StartLiveTail",
        "logs:StopLiveTail",
        "oam:ListSinks",
        "observabilityadmin:GetCentralizationRuleForOrganization",
        "observabilityadmin:ListCentralizationRulesForOrganization",
        "observabilityadmin:GetTelemetryEvaluationStatus",
        "observabilityadmin:GetTelemetryEvaluationStatusForOrganization",
        "observabilityadmin:GetTelemetryRule",
        "observabilityadmin:GetTelemetryRuleForOrganization",
        "observabilityadmin:ListResourceTelemetry",
        "observabilityadmin:ListResourceTelemetryForOrganization",
        "observabilityadmin:ListTelemetryRules",
        "observabilityadmin:ListTelemetryRulesForOrganization",
        "observabilityadmin:GetTelemetryEnrichmentStatus",
        "observabilityadmin:ListTagsForResource",
        "observabilityadmin:GetTelemetryPipeline",
        "observabilityadmin:ListTelemetryPipelines",
        "observabilityadmin:TestTelemetryPipeline",
        "observabilityadmin:ValidateTelemetryPipelineConfiguration",
        "observabilityadmin:GetS3TableIntegration",
        "observabilityadmin:ListS3TableIntegrations",
        "sns:Get*",
        "sns:List*",
        "rum:BatchGet*",
        "rum:Get*",
        "rum:List*",
        "synthetics:Describe*",
        "synthetics:Get*",
        "synthetics:List*",
        "xray:BatchGet*",
        "xray:Get*",
        "xray:List*",
        "xray:StartTraceRetrieval",
        "xray:CancelTraceRetrieval"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OAMReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "oam:ListAttachedLinks"
```

```
      ],
      "Resource" : "arn:aws:oam:*:*:sink/*"
    },
    {
      "Sid" : "CloudWatchReadOnlyGetRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/application-
signals.cloudwatch.amazonaws.com/AWSServiceRoleForCloudWatchApplicationSignals"
    },
    {
      "Sid" : "CloudWatchCloudTrailPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:GetChannel"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:channel/aws-service-channel/application-
signals/*"
    },
    {
      "Sid" : "CloudWatchServiceQuotaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : [
        "arn:aws:servicequotas:*:*:s3/*",
        "arn:aws:servicequotas:*:*:dynamodb/*",
        "arn:aws:servicequotas:*:*:kinesis/*",
        "arn:aws:servicequotas:*:*:sns/*",
        "arn:aws:servicequotas:*:*:bedrock/*",
        "arn:aws:servicequotas:*:*:lambda/*",
        "arn:aws:servicequotas:*:*:fargate/*",
        "arn:aws:servicequotas:*:*:elasticloadbalancing/*",
        "arn:aws:servicequotas:*:*:ec2/*"
      ]
    },
    {
      "Sid" : "CloudWatchResourceExplorerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:Search"
      ],
```

```
      "Resource" : [
        "arn:aws:resource-explorer-2:*::view/AWSServiceViewForApplicationSignals/
service-view",
        "arn:aws:resource-explorer-2:*::view/
AWSServiceViewForApplicationSignalsOrgScopeProd/service-view"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

CloudWatchSyntheticsFullAccess

説明: CloudWatch Synthetics へのフルアクセスを提供します。

`CloudWatchSyntheticsFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `CloudWatchSyntheticsFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 11 月 25 日 17:39 UTC
- 編集日時: 2024 年 11 月 21 日 22:21 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchSyntheticsFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v11 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "synthetics:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutEncryptionConfiguration"
      ],
      "Resource" : [
        "arn:aws:s3:::cw-syn-results-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "s3:ListAllMyBuckets",
        "xray:GetTraceSummaries",
        "xray:BatchGetTraces",
        "apigateway:GET"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation"
      ],
      "Resource" : "arn:aws:s3:::*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::cw-syn-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::aws-synthetics-library-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/CloudWatchSyntheticsRole*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lambda.amazonaws.com",
            "synthetics.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/CloudWatchSyntheticsRole*"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:Synthetics-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:GetLogRecord",
        "logs:DescribeLogStreams",
        "logs:StartQuery",
        "logs:GetLogEvents",
        "logs:FilterLogEvents",
        "logs:GetLogGroupFields"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/lambda/cwsyn-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:AddPermission",
        "lambda:PublishVersion",
        "lambda:UpdateFunctionCode",
        "lambda:UpdateFunctionConfiguration",
        "lambda:GetFunctionConfiguration",
        "lambda:GetFunction",
        "lambda:DeleteFunction",
        "lambda:ListTags",
        "lambda:TagResource",
        "lambda:UntagResource"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:cwsyn-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetLayerVersion",
        "lambda:PublishLayerVersion",
        "lambda:DeleteLayerVersion"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:layer:cwsyn-*",
        "arn:aws:lambda:*:*:layer:Synthetics:*",
        "arn:aws:lambda:*:*:layer:Synthetics_Selenium:*",
        "arn:aws:lambda:*:*:layer:AWS-CW-Synthetics*:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : [
        "*"
      ]
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:Subscribe",
        "sns:ListSubscriptionsByTopic"
      ],
      "Resource" : [
        "arn:*:sns:*:*:Synthetics-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
```

```
            "s3.*.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

CloudWatchSyntheticsReadOnlyAccess

説明: CloudWatch Synthetics への読み取り専用アクセスを提供します。

`CloudWatchSyntheticsReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `CloudWatchSyntheticsReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 11 月 25 日 17:45 UTC
- 編集日時: 2020 年 3 月 6 日 19:26 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchSyntheticsReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "synthetics:Describe*",
        "synthetics:Get*",
        "synthetics:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

ComprehendDataAccessRolePolicy

説明: データアクセスのために S3 リソースへのアクセスを許可する AWS Comprehend サービスロールのポリシー

`ComprehendDataAccessRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `ComprehendDataAccessRolePolicy` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2019 年 3 月 6 日 22:28 UTC
- 編集日時: 2019 年 3 月 6 日 22:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ComprehendDataAccessRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "s3:GetObject",
      "s3:ListBucket",
      "s3:PutObject"
    ],
    "Resource" : [
      "arn:aws:s3:::*Comprehend*",
      "arn:aws:s3:::*comprehend*"
    ]
  }
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

ComprehendFullAccess

説明: Amazon Comprehend へのフルアクセスを提供します。

ComprehendFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに ComprehendFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 11 月 29 日 18:08 UTC
- 編集日時: 2017 年 12 月 5 日 01:36 UTC
- ARN: arn:aws:iam::aws:policy/ComprehendFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "comprehend:*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketLocation",
```

```
        "iam:ListRoles",
        "iam:GetRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

ComprehendMedicalFullAccess

説明: Amazon Comprehend Medical へのフルアクセスを提供します

`ComprehendMedicalFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `ComprehendMedicalFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 11 月 27 日 17:55 UTC
- 編集日時: 2018 年 11 月 27 日 17:55 UTC
- ARN: `arn:aws:iam::aws:policy/ComprehendMedicalFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "comprehendmedical:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

ComprehendReadOnly

説明: Amazon Comprehend への読み取り専用アクセスを提供します。

`ComprehendReadOnly` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `ComprehendReadOnly` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2017 年 11 月 29 日 18:10 UTC
- 編集日時: 2022 年 4 月 26 日 21:32 UTC
- ARN: arn:aws:iam::aws:policy/ComprehendReadOnly

ポリシーのバージョン

ポリシーのバージョン: v11 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

ComputeOptimizerAutomationServiceRolePolicy

説明: ComputeOptimizerAutomationServiceRolePolicy 管理ポリシーは、Compute Optimizer がユーザーに代わってアクションを実行できるようにするサービスにリンクされたロールにアタッチされます。

ComputeOptimizerAutomationServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2025 年 11 月 15 日 01:19 UTC
- 編集日時: 2025 年 11 月 15 日 01:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ComputeOptimizerAutomationServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EBSReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumesModifications"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EBSVolumeModification",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:ModifyVolume",
        "ec2:DeleteVolume"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/exclude-from-compute-optimizer-automation" : "true"
        }
      }
    },
    {
      "Sid" : "CreateEBSSnapshot",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RollbackEBSVolumeDeletion",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "Tag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "ec2:CreateAction" : [
            "CreateVolume",
            "CreateSnapshot"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

ComputeOptimizerReadOnlyAccess

説明: ComputeOptimizer への読み取り専用アクセスを提供します。

`ComputeOptimizerReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `ComputeOptimizerReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 3 月 7 日 00:11 UTC
- 編集日時: 2024 年 11 月 20 日 21:08 UTC
- ARN: `arn:aws:iam::aws:policy/ComputeOptimizerReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v9 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "computeOptimizerReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "compute-optimizer:DescribeRecommendationExportJobs",
        "compute-optimizer:GetEnrollmentStatus",
        "compute-optimizer:GetEnrollmentStatusesForOrganization",
        "compute-optimizer:GetRecommendationSummaries",
        "compute-optimizer:GetEC2InstanceRecommendations",
        "compute-optimizer:GetEC2RecommendationProjectedMetrics",
        "compute-optimizer:GetAutoScalingGroupRecommendations",
        "compute-optimizer:GetEBSVolumeRecommendations",
        "compute-optimizer:GetLambdaFunctionRecommendations",
        "compute-optimizer:GetRecommendationPreferences",
        "compute-optimizer:GetEffectiveRecommendationPreferences",
        "compute-optimizer:GetECSServiceRecommendations",
        "compute-optimizer:GetECSServiceRecommendationProjectedMetrics",
        "compute-optimizer:GetRDSDatabaseRecommendations",
        "compute-optimizer:GetRDSDatabaseRecommendationProjectedMetrics",
        "compute-optimizer:GetLicenseRecommendations",
        "compute-optimizer:GetIdleRecommendations",
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ecs:ListServices",
        "ecs:ListClusters",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "lambda:ListFunctions",
        "lambda:ListProvisionedConcurrencyConfigs",
        "cloudwatch:GetMetricData",
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

ComputeOptimizerServiceRolePolicy

説明: ComputeOptimizer がユーザーに代わって AWS サービスを呼び出し、ワークロードの詳細を収集できるようにします。

`ComputeOptimizerServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 12 月 3 日 08:45 UTC
- 編集日時: 2025 年 11 月 19 日 01:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ComputeOptimizerServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ComputeOptimizerFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "compute-optimizer:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AwsOrgsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CloudWatchAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AutoScalingAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribePolicies",
        "autoscaling:DescribeScheduledActions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Ec2Access",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ec2:DescribeNatGateways",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

ConfigConformsServiceRolePolicy

説明: AWSConfig がコンフォーマンスパックを作成するために必要とするポリシー

`ConfigConformsServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー

- 作成日時: 2019 年 7 月 25 日 21:38 UTC
- 編集日時: 2023 年 1 月 12 日 04:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ConfigConformsServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
```

```
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

ConsoleFullAccessFromVercel

説明: Vercel Marketplace との統合を通じて作成されたアカウントで使用します AWS。Vercel Marketplace と統合されているサービスのすべてのリソースを管理するためのアクセスを提供します。

`ConsoleFullAccessFromVercel` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `ConsoleFullAccessFromVercel` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 12 月 11 日 16:49 UTC
- 編集日時: 2025 年 12 月 11 日 16:49 UTC
- ARN: `arn:aws:iam::aws:policy/ConsoleFullAccessFromVercel`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DSQL",
      "Effect" : "Allow",
      "Action" : [
        "dsql:GetCluster",
        "dsql:ListClusters",
        "dsql:ListTagsForResource",
        "dsql:UpdateCluster",
        "dsql:DbConnectAdmin",
        "dsql:DbConnect"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DynamoDB",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:BatchGetItem",
        "dynamodb:BatchWriteItem",
        "dynamodb:UpdateTimeToLive",
        "dynamodb:ConditionCheckItem",
        "dynamodb:UntagResource",
        "dynamodb:PutItem",
        "dynamodb:ListTables",
        "dynamodb:DeleteItem",
        "dynamodb:Scan",
        "dynamodb:ListTagsOfResource",
        "dynamodb:Query",
        "dynamodb:UpdateItem",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:TagResource",
        "dynamodb:DescribeTable",
        "dynamodb:GetItem",
        "dynamodb:DescribeLimits",
        "dynamodb:UpdateTable",
        "dynamodb:GetRecords"
      ],
      "Resource" : [
        "*"
      ]
```

```
    },
    {
      "Sid" : "Aurora",
      "Effect" : "Allow",
      "Action" : [
        "rds-db:connect",
        "rds:Describe*",
        "rds:ListTagsForResource",
        "rds:RebootDBInstance",
        "rds:DeleteDBInstance",
        "rds:StartDBInstance",
        "rds:ModifyDBInstance",
        "rds:ApplyPendingMaintenanceAction",
        "rds:StartDBCluster",
        "rds:DeleteDBCluster",
        "rds:RebootDBCluster",
        "rds:CreateDBClusterEndpoint",
        "rds:ModifyDBClusterEndpoint",
        "rds:ModifyDBCluster",
        "rds:DeleteDBClusterEndpoint",
        "rds:FailoverDBCluster",
        "rds:DeleteDBClusterParameterGroup",
        "rds:ModifyDBClusterParameterGroup",
        "rds:CopyDBClusterParameterGroup",
        "rds:ResetDBClusterParameterGroup",
        "rds:CreateDBClusterParameterGroup",
        "rds:ResetDBParameterGroup",
        "rds:ModifyDBParameterGroup",
        "rds:CopyDBParameterGroup",
        "rds:DeleteDBParameterGroup",
        "rds:CreateDBParameterGroup",
        "rds:DeleteDBClusterAutomatedBackup",
        "rds:CopyDBClusterSnapshot",
        "rds:RestoreDBClusterToPointInTime",
        "rds:RestoreDBClusterFromSnapshot",
        "rds:CreateDBClusterSnapshot",
        "rds:DeleteDBClusterSnapshot",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
```

```
      "Sid" : "AuroraRestricted",
      "Effect" : "Allow",
      "Action" : [
        "rds:CreateDBInstance"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "rds:DatabaseEngine" : "aurora-postgresql"
        }
      }
    },
    {
      "Sid" : "Observability",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:PutMetricAlarm",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "tag:GetTagKeys",
        "tag:GetTagValues"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ApplicationAutoscalingIntegration",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "application-autoscaling:service-namespace" : "dynamodb"
        }
      }
    },
    {
      "Sid" : "ApplicationAutoscalingDescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ViewFreeTierState",
      "Effect" : "Allow",
      "Action" : [
        "freetier:GetAccountPlanState"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

ConsoleViewOnlyAccessFromVercel

説明: Vercel Marketplace との統合を通じて作成されたアカウントで使用します AWS。Vercel Marketplace と統合されているサービスのすべてのリソースを表示するアクセスを提供します。

`ConsoleViewOnlyAccessFromVercel` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに ConsoleViewOnlyAccessFromVercel をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 12 月 11 日 16:49 UTC
- 編集日時: 2025 年 12 月 11 日 16:49 UTC
- ARN: arn:aws:iam::aws:policy/ConsoleViewOnlyAccessFromVercel

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DSQL",
      "Effect" : "Allow",
      "Action" : [
        "dsql:GetCluster",
        "dsql:ListClusters",
        "dsql:ListTagsForResource"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DynamoDB",
      "Effect" : "Allow",
```

```
      "Action" : [
        "dynamodb:ListTables",
        "dynamodb:ListTagsOfResource",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeLimits"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "Aurora",
      "Effect" : "Allow",
      "Action" : [
        "rds:Describe*",
        "rds:ListTagsForResource",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "Observability",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "tag:GetTagKeys",
        "tag:GetTagValues"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ApplicationAutoscalingDescribeActions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

CostOptimizationHubAdminAccess

説明: このマネージドポリシーは、Cost Optimization Hub への管理者アクセスを提供します。

`CostOptimizationHubAdminAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `CostOptimizationHubAdminAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 12 月 19 日 00:03 UTC
- 編集日時: 2025 年 11 月 19 日 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/CostOptimizationHubAdminAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CostOptimizationHubAdminAccess",
      "Effect" : "Allow",
      "Action" : [
        "cost-optimization-hub:ListEnrollmentStatuses",
        "cost-optimization-hub:UpdateEnrollmentStatus",
        "cost-optimization-hub:GetPreferences",
        "cost-optimization-hub:UpdatePreferences",
        "cost-optimization-hub:GetRecommendation",
        "cost-optimization-hub:ListRecommendations",
        "cost-optimization-hub:ListRecommendationSummaries",
        "cost-optimization-hub:ListEfficiencyMetrics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCreationOfServiceLinkedRoleForCostOptimizationHub",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/cost-optimization-hub.bcm.amazonaws.com/
AWSServiceRoleForCostOptimizationHub"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "cost-optimization-hub.bcm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowAWSServiceAccessForCostOptimizationHub",
      "Effect" : "Allow",
```

```
      "Action" : [
        "organizations:EnableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "organizations:ServicePrincipal" : [
            "cost-optimization-hub.bcm.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

CostOptimizationHubReadOnlyAccess

説明: このマネージドポリシーは、Cost Optimization Hub への読み取り専用アクセスを提供します。

`CostOptimizationHubReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `CostOptimizationHubReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 12 月 13 日 18:04 UTC
- 編集日時: 2025 年 11 月 19 日 16:49 UTC

- ARN: `arn:aws:iam::aws:policy/CostOptimizationHubReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CostOptimizationHubReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "cost-optimization-hub:ListEnrollmentStatuses",
        "cost-optimization-hub:GetPreferences",
        "cost-optimization-hub:GetRecommendation",
        "cost-optimization-hub:ListRecommendations",
        "cost-optimization-hub:ListRecommendationSummaries",
        "cost-optimization-hub:ListEfficiencyMetrics"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

CostOptimizationHubServiceRolePolicy

説明: Cost Optimization Hub が組織情報を取得し、最適化関連のデータとメタデータを収集できるようにします。

CostOptimizationHubServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 11 月 26 日 08:03 UTC
- 編集日時: 2025 年 7 月 17 日 18:07 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/CostOptimizationHubServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AwsOrgsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
```

```
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListParents",
        "organizations:DescribeOrganizationalUnit"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AwsOrgsScopedAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "organizations:ServicePrincipal" : [
            "cost-optimization-hub.bcm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CostExplorerAccess",
      "Effect" : "Allow",
      "Action" : [
        "ce:ListCostAllocationTags",
        "ce:GetCostAndUsage",
        "ce:GetDimensionValues"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

CustomerProfilesServiceLinkedRolePolicy

説明: Amazon Connect Customer Profiles がユーザーに代わって AWS サービスとリソースにアクセスできるようにします。

CustomerProfilesServiceLinkedRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 3 月 7 日 22:56 UTC
- 編集日時: 2024 年 11 月 26 日 22:21 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/CustomerProfilesServiceLinkedRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/CustomerProfiles"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/profile.amazonaws.com/
AWSServiceRoleForProfile_*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "connect-campaigns:PutProfileOutboundRequestBatch"
      ],
      "Resource" : [
        "arn:aws:connect-campaigns:*:*:campaign/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "profile:BatchGetProfile"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

DatabaseAdministrator

説明: AWS データベース AWS サービスのセットアップと設定に必要なサービスとアクションへのフルアクセス許可を付与します。

DatabaseAdministrator は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに DatabaseAdministrator をアタッチできます。

ポリシーの詳細

- タイプ: ジョブ機能ポリシー
- 作成日時: 2016 年 11 月 10 日 17:25 UTC
- 編集日時: 2025 年 10 月 1 日 17:19 UTC
- ARN: arn:aws:iam::aws:policy/job-function/DatabaseAdministrator

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:Describe*",
        "cloudwatch:DisableAlarmActions",
        "cloudwatch:EnableAlarmActions",
        "cloudwatch:Get*",
        "cloudwatch:List*",
```

```
        "cloudwatch:PutMetricAlarm",
        "datapipeline:ActivatePipeline",
        "datapipeline:CreatePipeline",
        "datapipeline:DeletePipeline",
        "datapipeline:DescribeObjects",
        "datapipeline:DescribePipelines",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:ListPipelines",
        "datapipeline:PutPipelineDefinition",
        "datapipeline:QueryObjects",
        "dynamodb:*",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "elasticache:*",
        "iam:ListRoles",
        "iam:GetRole",
        "kms:ListKeys",
        "lambda:CreateEventSourceMapping",
        "lambda:CreateFunction",
        "lambda:DeleteEventSourceMapping",
        "lambda:DeleteFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:ListEventSourceMappings",
        "lambda:ListFunctions",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:FilterLogEvents",
        "logs:GetLogEvents",
        "logs:Create*",
        "logs:PutLogEvents",
        "logs:PutMetricFilter",
        "pi:CreatePerformanceAnalysisReport",
        "pi:DeletePerformanceAnalysisReport",
        "pi:DescribeDimensionKeys",
        "pi:GetDimensionKeyDetails",
        "pi:GetPerformanceAnalysisReport",
        "pi:GetResourceMetadata",
        "pi:GetResourceMetrics",
        "pi:ListAvailableResourceDimensions",
```

```
        "pi:ListAvailableResourceMetrics",
        "pi:ListPerformanceAnalysisReports",
        "pi:ListTagsForResource",
        "pi:TagResource",
        "pi:UntagResource",
        "rds:*",
        "redshift:*",
        "s3:CreateBucket",
        "sns:CreateTopic",
        "sns:DeleteTopic",
        "sns:Get*",
        "sns:List*",
        "sns:SetTopicAttributes",
        "sns:Subscribe",
        "sns:Unsubscribe"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject*",
        "s3:Get*",
        "s3:List*",
        "s3:PutAccelerateConfiguration",
        "s3:PutBucketTagging",
        "s3:PutBucketVersioning",
        "s3:PutBucketWebsite",
        "s3:PutLifecycleConfiguration",
        "s3:PutReplicationConfiguration",
        "s3:PutObject*",
        "s3:Replicate*",
        "s3:RestoreObject"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
```

```
      "Resource" : [
        "arn:aws:iam::*:role/rds-monitoring-role",
        "arn:aws:iam::*:role/rdbms-lambda-access",
        "arn:aws:iam::*:role/lambda_exec_role",
        "arn:aws:iam::*:role/lambda-dynamodb-*",
        "arn:aws:iam::*:role/lambda-vpc-execution-role",
        "arn:aws:iam::*:role/DataPipelineDefaultRole",
        "arn:aws:iam::*:role/DataPipelineDefaultResourceRole"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

DataScientist

説明: AWS データ分析サービスにアクセス許可を付与します。

`DataScientist` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `DataScientist` をアタッチできます。

ポリシーの詳細

- タイプ: ジョブ機能ポリシー
- 作成日時: 2016 年 11 月 10 日 17:28 UTC
- 編集日時: 2019 年 12 月 3 日 16:48 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/DataScientist`

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

DAXServiceRolePolicy

説明: このポリシーにより、DAX が顧客に代わってネットワークインターフェイス、セキュリティグループ、サブネット、VPC を作成および管理できます。

DAXServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 3 月 5 日 17:51 UTC
- 編集日時: 2018 年 3 月 5 日 17:51 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/DAXServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

DeclarativePoliciesEC2Report

説明: EC2 宣言型ポリシーアカウントステータスレポートの実行に必要な読み取り専用 API へのアクセスを提供します。

`DeclarativePoliciesEC2Report` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー

- 作成日時: 2024 年 11 月 30 日 13:21 UTC
- 編集日時: 2024 年 11 月 30 日 13:21 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DeclarativePoliciesEC2Report`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DeclarativePoliciesEC2Report",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeRegions",
        "ec2:GetSerialConsoleAccessStatus",
        "ec2:GetInstanceMetadataDefaults",
        "ec2:GetImageBlockPublicAccessState",
        "ec2:GetSnapshotBlockPublicAccessState",
        "ec2:GetAllowedImagesSettings",
        "ec2:DescribeVpcBlockPublicAccessOptions"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する

- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

DynamoDBCloudWatchContributorInsightsServiceRolePolicy

説明: Amazon DynamoDB の Amazon CloudWatch Contributor Insights をサポートするために必要な許可。

DynamoDBCloudWatchContributorInsightsServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 11 月 15 日 21:13 UTC
- 編集日時: 2019 年 11 月 15 日 21:13 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/DynamoDBCloudWatchContributorInsightsServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

DynamoDBGlobalTableSettingsManagementServiceRolePolicy

説明: グローバルテーブルレプリカ設定を管理するために DynamoDB が必要とするアクセス許可

DynamoDBGlobalTableSettingsManagementServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2025 年 10 月 15 日 17:34 UTC

- 編集日時: 2025 年 11 月 22 日 01:19 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/DynamoDBGlobalTableSettingsManagementServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DynamoDBActionsNeededToReplicateSettings",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:RegisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget"
      ],
      "Resource" : [
        "arn:aws:application-autoscaling:*:*:scalable-target/*",
        "arn:aws:autoscaling:*:*:scalingPolicy:*:resource/dynamodb/table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "application-autoscaling:service-namespace" : [
            "dynamodb"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "DynamoDBReplicationServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "dynamodb.application-autoscaling.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

DynamoDBKinesisReplicationServiceRolePolicy

説明: KinesisDataStreams への Provide AWS DynamoDB アクセス

`DynamoDBKinesisReplicationServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 11 月 12 日 00:43 UTC
- 編集日時: 2020 年 11 月 12 日 00:43 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/DynamoDBKinesisReplicationServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する

- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

DynamoDBReplicationServiceRolePolicy

説明: DynamoDB がクロスリージョンデータのレプリケーションを行うために必要な許可

DynamoDBReplicationServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 11 月 9 日 23:55 UTC
- 編集日時: 2024 年 1 月 8 日 20:10 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/DynamoDBReplicationServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する

- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

EC2FastLaunchFullAccess

説明: このポリシーは EC2 Fast Launch アクションへのフルアクセスを許可します

EC2FastLaunchFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに EC2FastLaunchFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 5 月 13 日 22:45 UTC
- 編集日時: 2025 年 5 月 14 日 16:37 UTC
- ARN: arn:aws:iam::aws:policy/EC2FastLaunchFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2FastLaunch",
      "Effect" : "Allow",
      "Action" : [
        "ec2:EnableFastLaunch",
        "ec2:DisableFastLaunch",
        "ec2:DescribeFastLaunchImages"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2ReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes",
        "ec2:DescribeRegions",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeInstances",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeTags",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeAccountAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2CreateVPC",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpc"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
        },
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EC2ModifyDeleteVPC",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:DeleteVpc",
        "ec2:CreateSubnet",
        "ec2:ModifyVpcAttribute",
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        },
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EC2CreateSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSubnet"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
        },
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EC2DeleteSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSubnet"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        },
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EC2CreateSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
        },
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EC2ManageSecurityGroupEgress",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupEgress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        },
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : "ec2fastlaunch.amazonaws.com"
```

```
        }
      }
    },
    {
      "Sid" : "EC2DeleteSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        },
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudFormation",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack",
        "cloudformation:RollbackStack",
        "cloudformation:DeleteStack",
        "cloudformation:UpdateTerminationProtection",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/EC2FastLaunch*/*"
      ],
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
```

```
    {
      "Sid" : "EC2LaunchTemplateModify",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyLaunchTemplate",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
        },
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EC2LaunchInstance",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:license-manager:*:*:license-configuration:*"
      ]
    },
    {
      "Sid" : "EC2LaunchInstanceWithVolAndInstance",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    },
    {
      "Sid" : "EC2Tags",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "RunInstances"
        }
      }
    },
    {
      "Sid" : "EC2ManageTags",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
        },
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
```

```
      "Resource" : "arn:aws:iam::*:role/aws-service-role/ec2fastlaunch.amazonaws.com/
AWSServiceRoleForEC2FastLaunch",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMSLRPassRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:instance-profile/*",
        "arn:aws:iam::*:role/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

EC2FastLaunchServiceRolePolicy

説明: ポリシーは、ec2fastlaunch に、顧客のアカウントでプロビジョニングされたスナップショットの準備および管理と関連するメトリクスの公開を許可します。

EC2FastLaunchServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 1 月 10 日 13:08 UTC
- 編集日時: 2025 年 7 月 18 日 00:37 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/EC2FastLaunchServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowRunInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:key-pair/*",
```

```
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:license-manager:*:*:license-configuration:*"
      ]
    },
    {
      "Sid" : "AllowRunInstancesOnFastLaunchCreatedResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    },
    {
      "Sid" : "AllowPassRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Sid" : "AllowStopAndTerminateInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    },
    {
      "Sid" : "AllowCreateSnapshot",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshot",
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    },
    {
      "Sid" : "AllowCreateTaggedSnapshot",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshot",
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
        },
        "StringLike" : {
          "aws:RequestTag/CreatedByLaunchTemplateVersion" : "*"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "CreatedByLaunchTemplateName",
            "CreatedByLaunchTemplateId"
          ]
        }
      }
    },
    {
      "Sid" : "AllowCreateLaunchTemplate",
```

```
      "Effect" : "Allow",
      "Action" : "ec2:CreateLaunchTemplate",
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    },
    {
      "Sid" : "AllowCreateTags",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateSnapshot",
            "RunInstances",
            "CreateLaunchTemplate"
          ]
        }
      }
    },
    {
      "Sid" : "AllowDeleteSnapshots",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    },
```

```
    {
      "Sid" : "AllowDeleteVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    },
    {
      "Sid" : "AllowDeleteNetworkInterfaces",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    },
    {
      "Sid" : "AllowDescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeVolumes",
```

```
        "ec2:DescribeNetworkInterfaces",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowPutMetricData",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/EC2"
        }
      }
    },
    {
      "Sid" : "AllowEventsRuleMutations",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:PutRule",
        "events:PutTargets"
      ],
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "ec2fastlaunch.amazonaws.com"
        }
      },
      "Resource" : [
        "arn:aws:events:*:*:rule/FastLaunch*"
      ]
    },
    {
      "Sid" : "AllowEventsRuleNonMutations",
      "Effect" : "Allow",
      "Action" : [
        "events:ListTargetsByRule",
        "events:DescribeRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/FastLaunch*"
      ]
```

```
    },
    {
      "Sid" : "AllowKMSActions",
      "Effect" : "Allow",
      "Action" : "kms:ListRetirableGrants",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowDeleteFastLaunchLaunchTemplates",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteLaunchTemplate"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

EC2FleetTimeShiftableServiceRolePolicy

説明: EC2 フリートに今後インスタンスを起動するアクセス許可を付与するポリシー。

`EC2FleetTimeShiftableServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 12 月 23 日 19:47 UTC
- 編集日時: 2019 年 12 月 23 日 19:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/EC2FleetTimeShiftableServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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" : "*"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

Ec2ImageBuilderCrossAccountDistributionAccess

説明: EC2 Image Builder がアカウント間のディストリビューションを実行するために必要な許可です。

`Ec2ImageBuilderCrossAccountDistributionAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `Ec2ImageBuilderCrossAccountDistributionAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 9 月 30 日 19:22 UTC
- 編集日時: 2020 年 9 月 30 日 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/Ec2ImageBuilderCrossAccountDistributionAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

EC2ImageBuilderLifecycleExecutionPolicy

説明: EC2ImageBuilderLifecycleExecutionPolicy ポリシーは、イメージライフサイクル管理タスクの自動ルールをサポートするために、Image Builder イメージリソースとその基盤リソース (AMI、スナップショット) の非推奨化、または削除などのアクションを実行する権限を Image Builder に付与します。

`EC2ImageBuilderLifecycleExecutionPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `EC2ImageBuilderLifecycleExecutionPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 11 月 16 日 23:23 UTC
- 編集日時: 2023 年 11 月 16 日 23:23 UTC

- ARN: arn:aws:iam::aws:policy/service-role/EC2ImageBuilderLifecycleExecutionPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

EC2InstanceConnect

説明: お客様が EC2 Instance Connect を呼び出して EC2 インスタンスにエフェメラルキーを公開し、ssh または EC2 Instance Connect CLI 経由で接続できるようにします。

`EC2InstanceConnect` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `EC2InstanceConnect` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 6 月 27 日 18:53 UTC
- 編集日時: 2019 年 6 月 27 日 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/EC2InstanceConnect`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2InstanceConnect",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2-instance-connect:SendSSHPublicKey"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

Ec2InstanceConnectEndpoint

説明: 顧客が作成した EC2 インスタンス Connect エンドポイントを管理する EC2 インスタンス Connect エンドポイントポリシー

`Ec2InstanceConnectEndpoint` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 1 月 24 日 20:19 UTC
- 編集日時: 2025 年 7 月 31 日 17:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Ec2InstanceConnectEndpoint`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:subnet/*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "InstanceConnectEndpointId"
          ]
        },
        "StringLike" : {
          "aws:RequestTag/InstanceConnectEndpointId" : [
            "eice-*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/InstanceConnectEndpointId" : [
            "eice-*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        },
```

```
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "InstanceConnectEndpointId"
          ]
        },
        "StringLike" : {
          "aws:RequestTag/InstanceConnectEndpointId" : [
            "eice-*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignIpv6Addresses",
        "ec2:UnassignIpv6Addresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/InstanceConnectEndpointId" : [
            "eice-*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:ModifyNetworkInterfaceAttribute",
      "Resource" : "arn:aws:ec2:*:*:security-group/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/InstanceConnectEndpointId" : [
            "eice-*"
          ]
        }
```

```
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

EC2InstanceProfileForImageBuilder

説明: Image Builder サービスの EC2 インスタンスプロファイル。

`EC2InstanceProfileForImageBuilder` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `EC2InstanceProfileForImageBuilder` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 12 月 1 日 19:08 UTC
- 編集日時: 2025 年 5 月 19 日 20:37 UTC
- ARN: `arn:aws:iam::aws:policy/EC2InstanceProfileForImageBuilder`

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateSnapshot",
          "aws:RequestTag/CreatedBy" : [
            "EC2 Image Builder"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*/*.ISO",
        "arn:aws:s3:::*/*.iso",
        "arn:aws:s3:::*/*.Iso"
      ],
      "Condition" : {
        "StringEquals" : {
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "imagebuilder:GetComponent",
        "imagebuilder:GetMarketplaceResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:imagebuilder:arn",
          "aws:CalledVia" : [
            "imagebuilder.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::ec2imagebuilder*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/imagebuilder/*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

EC2InstanceProfileForImageBuilderECRContainerBuilds

説明: EC2 Image Builder を使用してコンテナイメージを構築するための EC2 インスタンスプロファイル。このポリシーは、ユーザーが ECR イメージをアップロードするために広範な許可を付与します。

EC2InstanceProfileForImageBuilderECRContainerBuilds は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに EC2InstanceProfileForImageBuilderECRContainerBuilds をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 12 月 11 日 19:48 UTC
- 編集日時: 2020 年 12 月 11 日 19:48 UTC
- ARN: arn:aws:iam::aws:policy/EC2InstanceProfileForImageBuilderECRContainerBuilds

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

ECRReplicationServiceRolePolicy

説明: ECR レプリケーションによって使用または管理される AWS のサービス および リソースへのアクセスを有効にします

ECRReplicationServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 12 月 4 日 22:11 UTC
- 編集日時: 2020 年 12 月 4 日 22:11 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/ECRReplicationServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository",
        "ecr:ReplicateImage"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

ECRTemplateServiceRolePolicy

説明: AWS ECR リポジトリ作成テンプレートを使用する場合のアクションの実行を許可します

ECRTemplateServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2024 年 6 月 19 日 23:11 UTC
- 編集日時: 2024 年 6 月 19 日 23:11 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/ECRTemplateServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateRepositoryWithTemplate",
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

ElastiCacheServiceRolePolicy

説明: このポリシーにより、ElastiCache はキャッシュの管理に必要な AWS リソースをユーザーに代わって管理できます。

`ElastiCacheServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 12 月 7 日 17:50 UTC
- 編集日時: 2023 年 11 月 28 日 03:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ElastiCacheServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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/*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

ElasticLoadBalancingFullAccess

説明: Amazon ElasticLoadBalancing へのフルアクセスと、ElasticLoadBalancing 機能の提供に必要な他のサービスへの制限付きアクセスを提供します。

`ElasticLoadBalancingFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `ElasticLoadBalancingFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 9 月 20 日 20:42 UTC
- 編集日時: 2024 年 10 月 24 日 22:21 UTC
- ARN: `arn:aws:iam::aws:policy/ElasticLoadBalancingFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeRouteTables",
        "ec2:DescribeCoipPools",
        "ec2:GetCoipPoolUsage",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:DescribeVpcPeeringConnections",
        "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" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

ElasticLoadBalancingReadOnly

説明: Amazon Elastic Load Balancing および依存サービスへの読み取り専用アクセスを提供します

`ElasticLoadBalancingReadOnly` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `ElasticLoadBalancingReadOnly` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 9 月 20 日 20:17 UTC
- 編集日時: 2023 年 11 月 26 日 18:15 UTC
- ARN: `arn:aws:iam::aws:policy/ElasticLoadBalancingReadOnly`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

ElementalActivationsDownloadSoftwareAccess

説明: 購入したアセットを表示したり、関連ソフトウェアやキックスタートファイルをダウンロードするためのアクセス

`ElementalActivationsDownloadSoftwareAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `ElementalActivationsDownloadSoftwareAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2020 年 9 月 8 日 17:26 UTC
- 編集日時: 2020 年 9 月 8 日 17:26 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsDownloadSoftwareAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-activations:Get*",
        "elemental-activations:Download*"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

ElementalActivationsFullAccess

説明: Elemental Appliance および Software の購入済みアセットを閲覧してアクションを実行するためのフルアクセス

`ElementalActivationsFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `ElementalActivationsFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 6 月 4 日 21:00 UTC
- 編集日時: 2020 年 6 月 4 日 21:00 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-activations:*"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

ElementalActivationsGenerateLicenses

説明: 購入済みアセットの閲覧と、実施待ちアクティベーション向けソフトウェアライセンスを生成するためのアクセス

`ElementalActivationsGenerateLicenses` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `ElementalActivationsGenerateLicenses` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 8 月 28 日 18:28 UTC
- 編集日時: 2020 年 8 月 28 日 18:28 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsGenerateLicenses`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-activations:Get*",
        "elemental-activations:GenerateLicenses",
        "elemental-activations:StartFileUpload",
        "elemental-activations:CompleteFileUpload"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

ElementalActivationsReadOnlyAccess

説明: AWS アカウント ユーザーの に関連付けられた購入済みアセットの詳細なリストへの読み取り専用アクセス

`ElementalActivationsReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `ElementalActivationsReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 8 月 28 日 16:51 UTC
- 編集日時: 2020 年 8 月 28 日 16:51 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-activations:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

ElementalAppliancesSoftwareFullAccess

説明: Elemental アプライアンスとソフトウェアの見積もりおよび注文データの閲覧およびアクションを実行するためのフルアクセス

`ElementalAppliancesSoftwareFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `ElementalAppliancesSoftwareFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 7 月 31 日 16:28 UTC
- 編集日時: 2021 年 2 月 5 日 21:01 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalAppliancesSoftwareFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-appliances-software:*",
        "elemental-activations:CompleteAccountRegistration"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

ElementalAppliancesSoftwareReadOnlyAccess

説明: Elemental アプライアンスとソフトウェアの見積もりおよび注文データを閲覧する読み取り専用アクセス

`ElementalAppliancesSoftwareReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `ElementalAppliancesSoftwareReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 4 月 1 日 22:31 UTC
- 編集日時: 2020 年 4 月 1 日 22:31 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalAppliancesSoftwareReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-appliances-software:List*",
        "elemental-appliances-software:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

ElementalSupportCenterFullAccess

説明: Elemental アプライアンスとソフトウェアのサポートケースおよび製品サポートコンテンツの閲覧およびアクションを行うためのフルアクセス

`ElementalSupportCenterFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `ElementalSupportCenterFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 11 月 25 日 18:08 UTC
- 編集日時: 2021 年 2 月 5 日 21:02 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalSupportCenterFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-support-cases:*",
        "elemental-support-content:*",
        "elemental-activations:CompleteAccountRegistration"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

EMRDescribeClusterPolicyForEMRWAL

説明: このポリシーは、Amazon EMR の WAL サービスがクラスターのステータスを検索して返すための読み取り専用許可を付与します。

EMRDescribeClusterPolicyForEMRWAL は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 6 月 15 日 23:30 UTC
- 編集日時: 2023 年 6 月 15 日 23:30 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/EMRDescribeClusterPolicyForEMRWAL

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:DescribeCluster"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

FMSServiceRolePolicy

説明: FM サービスにリンクされたロールが、お客様の AWS Organization アカウント内の FM マネージドリソースに対して FM 関連のアクションを実行することを許可するアクセスポリシー。

FMSServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 3 月 28 日 23:01 UTC
- 編集日時: 2025 年 5 月 21 日 18:22 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/FMSServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v32 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "WafGeneral",
      "Effect" : "Allow",
      "Action" : [
        "waf:UpdateWebACL",
        "waf:DeleteWebACL",
        "waf:GetWebACL",
        "waf:GetRuleGroup",
        "waf:ListSubscribedRuleGroups",
        "waf-regional:UpdateWebACL",
        "waf-regional:DeleteWebACL",
        "waf-regional:GetWebACL",
        "waf-regional:GetRuleGroup",
        "waf-regional:ListSubscribedRuleGroups",
        "waf-regional:ListResourcesForWebACL",
        "waf-regional:AssociateWebACL",
        "waf-regional:DisassociateWebACL",
        "elasticloadbalancing:SetWebACL",
        "apigateway:SetWebACL",
        "elasticloadbalancing:SetSecurityGroups",
        "waf:ListTagsForResource",
        "waf-regional:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:waf:*:*:webacl/*",
        "arn:aws:waf-regional:*:*:webacl/*",
        "arn:aws:waf:*:*:rulegroup/*",
        "arn:aws:waf-regional:*:*:rulegroup/*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*",
        "arn:aws:apigateway:*::/restapis/*/stages/*"
      ]
    },
    {
      "Sid" : "Wafv2Logging",
```

```
      "Effect" : "Allow",
      "Action" : [
        "wafv2:PutLoggingConfiguration",
        "wafv2:GetLoggingConfiguration",
        "wafv2:ListLoggingConfigurations",
        "wafv2:DeleteLoggingConfiguration"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:regional/webacl/*",
        "arn:aws:wafv2:*:*:global/webacl/*"
      ]
    },
    {
      "Sid" : "WafWebaclCreation",
      "Effect" : "Allow",
      "Action" : [
        "waf:CreateWebACL",
        "waf-regional:CreateWebACL",
        "waf:GetChangeToken",
        "waf-regional:GetChangeToken",
        "waf-regional:GetWebACLForResource"
      ],
      "Resource" : [
        "arn:aws:waf:*:*:*",
        "arn:aws:waf-regional:*:*:*"
      ]
    },
    {
      "Sid" : "ElbGeneral",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
        "elasticloadbalancing:DescribeTags"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "WafPermissionPolicy",
      "Effect" : "Allow",
      "Action" : [
        "waf:PutPermissionPolicy",
        "waf:GetPermissionPolicy",
        "waf:DeletePermissionPolicy",
        "waf-regional:PutPermissionPolicy",
```

```
        "waf-regional:GetPermissionPolicy",
        "waf-regional:DeletePermissionPolicy"
      ],
      "Resource" : [
        "arn:aws:waf:*:*:webacl/*",
        "arn:aws:waf:*:*:rulegroup/*",
        "arn:aws:waf-regional:*:*:webacl/*",
        "arn:aws:waf-regional:*:*:rulegroup/*"
      ]
    },
    {
      "Sid" : "CloudfrontGeneral",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:GetDistribution",
        "cloudfront:UpdateDistribution",
        "cloudfront:ListDistributionsByWebACLId",
        "cloudfront:ListDistributions",
        "cloudfront:ListTagsForResource",
        "cloudfront:AssociateDistributionWebACL",
        "cloudfront:DisassociateDistributionWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConfigScoped",
      "Effect" : "Allow",
      "Action" : [
        "config:DeleteConfigRule",
        "config:GetComplianceDetailsByConfigRule",
        "config:PutConfigRule",
        "config:StartConfigRulesEvaluation",
        "config:DeleteEvaluationResults"
      ],
      "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/fms.amazonaws.com/
*"
    },
    {
      "Sid" : "ConfigUnscoped",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeComplianceByConfigRule",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
```

```
        "config:DescribeConfigRules",
        "config:DescribeConfigRuleEvaluationStatus",
        "config:PutConfigurationRecorder",
        "config:StartConfigurationRecorder",
        "config:PutDeliveryChannel",
        "config:DescribeDeliveryChannels",
        "config:DescribeDeliveryChannelStatus",
        "config:GetComplianceSummaryByConfigRule",
        "config:GetDiscoveredResourceCounts",
        "config:PutEvaluations",
        "config:SelectResourceConfig",
        "config:BatchGetResourceConfig"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SlrDeletion",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/fms.amazonaws.com/AWSServiceRoleForFMS"
      ]
    },
    {
      "Sid" : "OrganizationsGeneral",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListChildren",
        "organizations:ListRoots",
        "organizations:ListParents",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : [
        "*"
      ]
    },
```

```
    {
      "Sid" : "ShieldGeneral",
      "Effect" : "Allow",
      "Action" : [
        "shield:CreateProtection",
        "shield:DeleteProtection",
        "shield:DescribeProtection",
        "shield:ListProtections",
        "shield:ListAttacks",
        "shield:CreateSubscription",
        "shield:DescribeSubscription",
        "shield:GetSubscriptionState",
        "shield:DescribeDRTAccess",
        "shield:DescribeEmergencyContactSettings",
        "shield:UpdateEmergencyContactSettings",
        "elasticloadbalancing:DescribeLoadBalancers",
        "ec2:DescribeAddresses",
        "shield:EnableApplicationLayerAutomaticResponse",
        "shield:DisableApplicationLayerAutomaticResponse",
        "shield:UpdateApplicationLayerAutomaticResponse"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2SecurityGroupScoped",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:UpdateSecurityGroupRuleDescriptionsEgress",
        "ec2:UpdateSecurityGroupRuleDescriptionsIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Sid" : "SecurityGroupTagCreation",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateSecurityGroup"
        }
      }
    },
    {
      "Sid" : "SecurityGroupTagManagement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteTags",
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/FMManaged" : "*"
        }
      }
    },
    {
      "Sid" : "Ec2Unscoped",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup",
        "ec2:DescribeSecurityGroupReferences",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeStaleSecurityGroups",
        "ec2:DescribeNetworkInterfaces",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeInstances",
        "ec2:AssociateRouteTable",
        "ec2:CreateSubnet",
```

```
        "ec2:CreateRouteTable",
        "ec2:DeleteSubnet",
        "ec2:DisassociateRouteTable",
        "ec2:ReplaceRouteTableAssociation"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "Wafv2General",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:TagResource",
        "wafv2:ListResourcesForWebACL",
        "wafv2:AssociateWebACL",
        "wafv2:ListTagsForResource",
        "wafv2:UntagResource",
        "wafv2:GetWebACL",
        "wafv2:DisassociateFirewallManager",
        "wafv2:DeleteWebACL",
        "wafv2:DisassociateWebACL"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:global/webacl/*",
        "arn:aws:wafv2:*:*:regional/webacl/*"
      ]
    },
    {
      "Sid" : "Wafv2WebAclAndRuleGroupMutation",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:UpdateWebACL",
        "wafv2:CreateWebACL",
        "wafv2:DeleteFirewallManagerRuleGroups",
        "wafv2:PutFirewallManagerRuleGroups"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:global/webacl/*",
        "arn:aws:wafv2:*:*:regional/webacl/*",
        "arn:aws:wafv2:*:*:global/rulegroup/*",
        "arn:aws:wafv2:*:*:regional/rulegroup/*",
        "arn:aws:wafv2:*:*:global/managedruleset/*",
        "arn:aws:wafv2:*:*:regional/managedruleset/*",
```

```
        "arn:aws:wafv2:*:*:global/ipset/*",
        "arn:aws:wafv2:*:*:regional/ipset/*",
        "arn:aws:wafv2:*:*:global/regexpatternset/*",
        "arn:aws:wafv2:*:*:regional/regexpatternset/*"
      ]
    },
    {
      "Sid" : "Wafv2PermissionPolicy",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:PutPermissionPolicy",
        "wafv2:GetPermissionPolicy",
        "wafv2:DeletePermissionPolicy"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:global/rulegroup/*",
        "arn:aws:wafv2:*:*:regional/rulegroup/*"
      ]
    },
    {
      "Sid" : "Wafv2WebaclDescribe",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:GetWebACLForResource"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:regional/webacl/*"
      ]
    },
    {
      "Sid" : "RouteTableTagManagement",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:route-table/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateRouteTable"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "SubnetTagManagement",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged"
          ]
        }
      }
    },
    {
      "Sid" : "VPCEndpointTagManagement",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged"
          ]
        }
      }
    },
    {
      "Sid" : "RouteTableCleanup",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteRouteTable",
      "Resource" : "arn:aws:ec2:*:*:route-table/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "ec2:ResourceTag/FMManaged" : "true"
        }
      }
    },
    {
      "Sid" : "Ec2DescribeUnscoped",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInternetGateways",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateVpcEndpointScoped",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/FMManaged" : [
            "true"
          ]
        }
      }
    },
    {
      "Sid" : "CreateVpcEndpointUnscoped",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "VpcEndpointsDeletion",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/FMManaged" : "true"
        }
      }
    },
    {
      "Sid" : "RamTagManagement",
      "Effect" : "Allow",
      "Action" : [
        "ram:TagResource"
      ],
      "Resource" : [
        "arn:aws:ram:*:*:resource-share/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged"
          ]
        }
      }
    },
    {
      "Sid" : "RamMutation",
      "Effect" : "Allow",
      "Action" : [
        "ram:AssociateResourceShare",
        "ram:UpdateResourceShare",
        "ram:DeleteResourceShare"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/FMManaged" : "true"
        }
      }
    },
    {
```

```
      "Sid" : "RamCreation",
      "Effect" : "Allow",
      "Action" : "ram:CreateResourceShare",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/FMManaged" : [
            "true"
          ]
        }
      }
    },
    {
      "Sid" : "RamDescribe",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShareAssociations",
        "ram:GetResourceShares"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SlrCreation",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "network-firewall.amazonaws.com",
            "shield.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "IamDescribe",
      "Effect" : "Allow",
```

```
      "Action" : "iam:GetRole",
      "Resource" : "*"
    },
    {
      "Sid" : "NetworkFirewallTagManagement",
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged"
          ]
        }
      }
    },
    {
      "Sid" : "NetworkFirewallGeneral",
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:AssociateSubnets",
        "network-firewall:CreateFirewall",
        "network-firewall:CreateFirewallPolicy",
        "network-firewall:DisassociateSubnets",
        "network-firewall:UpdateFirewallDeleteProtection",
        "network-firewall:UpdateFirewallPolicy",
        "network-firewall:UpdateFirewallPolicyChangeProtection",
        "network-firewall:UpdateSubnetChangeProtection",
        "network-firewall:AssociateFirewallPolicy",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DeleteResourcePolicy",
        "network-firewall:DescribeLoggingConfiguration",
        "network-firewall:UpdateLoggingConfiguration",
        "network-firewall:DescribeTLSInspectionConfiguration",
        "network-firewall:ListTLSInspectionConfigurations"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "NetworkFirewallResourcePolicy",
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:PutResourcePolicy"
      ],
      "Resource" : [
        "arn:aws:network-firewall:*:*:firewall-policy/*",
        "arn:aws:network-firewall:*:*:stateful-rulegroup/*",
        "arn:aws:network-firewall:*:*:stateless-rulegroup/*"
      ]
    },
    {
      "Sid" : "NetworkFirewallCleanup",
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:DeleteFirewallPolicy",
        "network-firewall:DeleteFirewall"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/FMManaged" : "true"
        }
      }
    },
    {
      "Sid" : "LogsGeneral",
      "Effect" : "Allow",
      "Action" : [
        "logs:ListLogDeliveries",
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Route53ResolverRuleGroupUnscoped",
      "Effect" : "Allow",
```

```
      "Action" : [
        "route53resolver:ListFirewallRuleGroupAssociations",
        "route53resolver:ListTagsForResource",
        "route53resolver:ListFirewallRuleGroups",
        "route53resolver:GetFirewallRuleGroupAssociation",
        "route53resolver:GetFirewallRuleGroup",
        "route53resolver:GetFirewallRuleGroupPolicy",
        "route53resolver:PutFirewallRuleGroupPolicy"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Route53ResolverRuleGroupCleanup",
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:UpdateFirewallRuleGroupAssociation",
        "route53resolver:DisassociateFirewallRuleGroup"
      ],
      "Resource" : "arn:aws:route53resolver:*:*:firewall-rule-group-association/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/FMManaged" : "true"
        }
      }
    },
    {
      "Sid" : "Route53ResolverRuleGroupScoped",
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:AssociateFirewallRuleGroup",
        "route53resolver:TagResource"
      ],
      "Resource" : "arn:aws:route53resolver:*:*:firewall-rule-group-association/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/FMManaged" : "true"
        }
      }
    },
    {
      "Sid" : "NaclTagCreation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
```

```
      ],
      "Resource" : "arn:aws:ec2:*:*:network-acl/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged",
            "FMPolicies"
          ]
        },
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkAcl"
        }
      }
    },
    {
      "Sid" : "NaclTagManagement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-acl/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged",
            "FMPolicies"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/FMManaged" : "true"
        }
      }
    },
    {
      "Sid" : "NaclScoped",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkAclEntry",
        "ec2:CreateNetworkAclEntry",
        "ec2:ReplaceNetworkAclEntry",
        "ec2:DeleteNetworkAcl"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/FMManaged" : "true"
        }
      }
    },
    {
      "Sid" : "NaclUnscoped",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ReplaceNetworkAclAssociation",
        "ec2:DescribeNetworkAcls",
        "ec2:CreateNetworkAcl"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

FSxDeleteServiceLinkedRoleAccess

説明: Amazon FSx が Amazon S3 アクセス用の サービスリンクロールを削除できるようにします

`FSxDeleteServiceLinkedRoleAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー

- 作成日時: 2018 年 11 月 28 日 10:40 UTC
- 編集日時: 2018 年 11 月 28 日 10:40 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/FSxDeleteServiceLinkedRoleAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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_*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

GameLiftContainerFleetPolicy

説明: Amazon S3 などの依存関係へのアクセスなど、Amazon GameLift コンテナフリートのコンピューティングアクションに必要なアクセス許可を付与します。

GameLiftContainerFleetPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに GameLiftContainerFleetPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 11 月 12 日 19:28 UTC
- 編集日時: 2025 年 2 月 5 日 20:37 UTC
- ARN: arn:aws:iam::aws:policy/GameLiftContainerFleetPolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "WriteGameSessionLogsToLogStream",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:gamelift-*:log-stream:*"
```

```
    },
    {
      "Sid" : "CreateLogGroupToStoreGameSessionLogs",
      "Effect" : "Allow",
      "Action" : "logs:CreateLogGroup",
      "Resource" : "arn:aws:logs:*:*:log-group:gamelift-*"
    },
    {
      "Sid" : "WriteGameSessionLogsToS3Bucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetBucketLocation"
      ],
      "Resource" : [
        "arn:aws:s3:::gamelift-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RetrieveComputeAuthToken",
      "Effect" : "Allow",
      "Action" : [
        "gamelift:GetComputeAuthToken"
      ],
      "Resource" : [
        "arn:aws:gamelift:*:*:containerfleet/*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

GameLiftGameServerGroupPolicy

説明: Gamelift GameServerGroup がカスタマーリソースを管理できるようにするポリシー

GameLiftGameServerGroupPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに GameLiftGameServerGroupPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 4 月 3 日 23:12 UTC
- 編集日時: 2020 年 5 月 13 日 17:27 UTC
- ARN: arn:aws:iam::aws:policy/GameLiftGameServerGroupPolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

GitLabDuoWithAmazonQPermissionsPolicy

説明: このマネージドポリシーは、Amazon Q に接続し、GitLab Duo with Amazon Q 統合の機能を利用するアクセス許可を付与します。

`GitLabDuoWithAmazonQPermissionsPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `GitLabDuoWithAmazonQPermissionsPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 4 月 16 日 16:37 UTC
- 編集日時: 2025 年 4 月 16 日 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/GitLabDuoWithAmazonQPermissionsPolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GitLabDuoUsagePermissions",
      "Effect" : "Allow",
      "Action" : [
        "q:SendEvent",
        "q:CreateAuthGrant",
        "q:UpdateAuthGrant",
        "q:GenerateCodeRecommendations",
        "q:SendMessage",
        "q:ListPlugins",
        "q:VerifyOAuthAppConnection"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GitLabDuoManagementPermissions",
      "Effect" : "Allow",
      "Action" : [
        "q:CreateOAuthAppConnection",
        "q:DeleteOAuthAppConnection"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GitLabDuoPluginPermissions",
      "Effect" : "Allow",
      "Action" : [
        "q:CreatePlugin",
        "q:DeletePlugin",
        "q:GetPlugin"
      ],
      "Resource" : "arn:aws:qdeveloper:*:*:plugin/GitLabDuoWithAmazonQ/*"
    }
  ]
```

```
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

GlobalAcceleratorFullAccess

説明: GlobalAccelerator ユーザーにすべての API へのフルアクセスを許可します

`GlobalAcceleratorFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `GlobalAcceleratorFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 11 月 27 日 02:44 UTC
- 編集日時: 2020 年 12 月 4 日 19:17 UTC
- ARN: `arn:aws:iam::aws:policy/GlobalAcceleratorFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

```
  "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"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

GlobalAcceleratorReadOnlyAccess

説明: GlobalAccelerator ユーザーに読み取り専用 API へのアクセスを許可します

`GlobalAcceleratorReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `GlobalAcceleratorReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 11 月 27 日 02:41 UTC
- 編集日時: 2018 年 11 月 27 日 02:41 UTC
- ARN: `arn:aws:iam::aws:policy/GlobalAcceleratorReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "globalaccelerator:Describe*",
        "globalaccelerator:List*"
```

```
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

GreengrassOTAUpdateArtifactAccess

説明: すべての Greengrass リージョン内の Greengrass OTA アップデートアーティファクトへの読み取りアクセスを提供します

`GreengrassOTAUpdateArtifactAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `GreengrassOTAUpdateArtifactAccess` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2017 年 11 月 29 日 18:11 UTC
- 編集日時: 2018 年 12 月 18 日 00:59 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/GreengrassOTAUpdateArtifactAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowsIotToAccessGreengrassOTAUpdateArtifacts",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*-greengrass-updates/*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

GroundTruthSyntheticConsoleFullAccess

説明: このポリシーは、SageMaker Ground Truth 合成コンソールのすべての機能を使用するために必要な許可を付与します。

`GroundTruthSyntheticConsoleFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに GroundTruthSyntheticConsoleFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 8 月 25 日 15:58 UTC
- 編集日時: 2022 年 8 月 25 日 15:58 UTC
- ARN: arn:aws:iam::aws:policy/GroundTruthSyntheticConsoleFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker-groundtruth-synthetic:*",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する

- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

GroundTruthSyntheticConsoleReadOnlyAccess

説明: このポリシーは、 を介して SageMaker Ground Truth Synthetic への読み取り専用アクセスを許可します AWS マネジメントコンソール。

`GroundTruthSyntheticConsoleReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `GroundTruthSyntheticConsoleReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 8 月 25 日 15:58 UTC
- 編集日時: 2022 年 8 月 25 日 15:58 UTC
- ARN: `arn:aws:iam::aws:policy/GroundTruthSyntheticConsoleReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "sagemaker-groundtruth-synthetic:List*",
        "sagemaker-groundtruth-synthetic:Get*",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

Health_OrganizationsServiceRolePolicy

説明:組織ビュー機能を有効にする AWS ヘルスポリシー

`Health_OrganizationsServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 12 月 16 日 13:28 UTC
- 編集日時: 2024 年 2 月 6 日 16:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Health_OrganizationsServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "HealthAPIOrganizationView0",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

IAMAccessAdvisorReadOnly

説明: このポリシーは、サービスへの最新アクセス情報など、IAM アクセスアドバイザーが提供するすべてのアクセス情報を読み取るためのアクセスを付与します。

IAMAccessAdvisorReadOnly は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに IAMAccessAdvisorReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 6 月 21 日 19:33 UTC
- 編集日時: 2019 年 6 月 21 日 19:33 UTC
- ARN: arn:aws:iam::aws:policy/IAMAccessAdvisorReadOnly

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

IAMAccessAnalyzerFullAccess

説明: IAM Access Analyzer へのフルアクセスを提供します

`IAMAccessAnalyzerFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `IAMAccessAnalyzerFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 12 月 2 日 17:12 UTC
- 編集日時: 2019 年 12 月 2 日 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/IAMAccessAnalyzerFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

IAMAccessAnalyzerReadOnlyAccess

説明: IAM Access Analyzer リソースへの読み取り専用アクセスを提供します

`IAMAccessAnalyzerReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `IAMAccessAnalyzerReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 12 月 2 日 17:12 UTC
- 編集日時: 2024 年 7 月 18 日 17:49 UTC
- ARN: `arn:aws:iam::aws:policy/IAMAccessAnalyzerReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IAMAccessAnalyzerReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:CheckAccessNotGranted",
        "access-analyzer:CheckNoNewAccess",
        "access-analyzer:CheckNoPublicAccess",
        "access-analyzer:Get*",
        "access-analyzer:List*",
        "access-analyzer:ValidatePolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

IAMFullAccess

説明: 経由で IAM へのフルアクセスを提供します AWS マネジメントコンソール。

`IAMFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに IAMFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2019 年 6 月 21 日 19:40 UTC
- ARN: arn:aws:iam::aws:policy/IAMFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

IAMReadOnlyAccess

説明: 経由で IAM への読み取り専用アクセスを提供します AWS マネジメントコンソール。

`IAMReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `IAMReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2018 年 1 月 25 日 19:11 UTC
- ARN: `arn:aws:iam::aws:policy/IAMReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GenerateCredentialReport",
        "iam:GenerateServiceLastAccessedDetails",
        "iam:Get*",
        "iam:List*",
        "iam:SimulateCustomPolicy",
        "iam:SimulatePrincipalPolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

IAMSelfManageServiceSpecificCredentials

説明: IAM ユーザーが独自のサービス固有の認証情報を管理できるようにします。

`IAMSelfManageServiceSpecificCredentials` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `IAMSelfManageServiceSpecificCredentials` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2016 年 12 月 22 日 17:25 UTC
- 編集日時: 2016 年 12 月 22 日 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/IAMSelfManageServiceSpecificCredentials`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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}"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

IAMUserChangePassword

説明: IAM ユーザーが自身のパスワードを変更できるようにします。

`IAMUserChangePassword` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `IAMUserChangePassword` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2016 年 11 月 15 日 00:25 UTC
- 編集日時: 2025 年 5 月 29 日 21:52 UTC
- ARN: `arn:aws:iam::aws:policy/IAMUserChangePassword`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ChangePassword"
      ],
```

```
      "Resource" : [
        "arn:aws:iam::*:user/${aws:username}",
        "arn:aws:iam::*:user/*/${aws:username}"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetAccountPasswordPolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

IAMUserSSHKeys

説明: IAM ユーザーが自身の SSH キーを管理できるようにします。

`IAMUserSSHKeys` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `IAMUserSSHKeys` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 7 月 9 日 17:08 UTC
- 編集日時: 2015 年 7 月 9 日 17:08 UTC
- ARN: `arn:aws:iam::aws:policy/IAMUserSSHKeys`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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}"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

IVSFullAccess

説明: インタラクティブビデオサービス (IVS) へのフルアクセスを提供します。また、ivs コンソールへのフルアクセスに必要な依存サービスへのアクセス許可も含まれています。

IVSFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに IVSFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 12 月 13 日 21:20 UTC
- 編集日時: 2023 年 12 月 13 日 21:20 UTC
- ARN: arn:aws:iam::aws:policy/IVSFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IVSFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "ivs:*",
        "ivschat:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

IVSReadOnlyAccess

説明: IVS Low-Latency and Real-Time ストリーミング API への読み取り専用アクセスを提供します

`IVSReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `IVSReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 12 月 5 日 18:00 UTC
- 編集日時: 2025 年 7 月 24 日 20:22 UTC
- ARN: `arn:aws:iam::aws:policy/IVSReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "IVSReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "ivs:BatchGetChannel",
        "ivs:GetChannel",
        "ivs:GetComposition",
        "ivs:GetEncoderConfiguration",
        "ivs:GetIngestConfiguration",
        "ivs:GetParticipant",
        "ivs:GetPlaybackKeyPair",
        "ivs:GetPlaybackRestrictionPolicy",
        "ivs:GetPublicKey",
        "ivs:GetRecordingConfiguration",
        "ivs:GetStage",
        "ivs:GetStageSession",
        "ivs:GetStorageConfiguration",
        "ivs:GetStream",
        "ivs:GetStreamSession",
        "ivs:ListChannels",
        "ivs:ListCompositions",
        "ivs:ListEncoderConfigurations",
        "ivs:ListIngestConfigurations",
        "ivs:ListParticipants",
        "ivs:ListParticipantReplicas",
        "ivs:ListParticipantEvents",
        "ivs:ListPlaybackKeyPairs",
        "ivs:ListPlaybackRestrictionPolicies",
        "ivs:ListPublicKeys",
        "ivs:ListRecordingConfigurations",
        "ivs:ListStages",
        "ivs:ListStageSessions",
        "ivs:ListStorageConfigurations",
        "ivs:ListStreamKeys",
        "ivs:ListStreams",
        "ivs:ListStreamSessions",
        "ivs:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

IVSRecordToS3

説明: IVS ライブストリームの録画に S3 PutObject を実行するための サービスリンクロール

`IVSRecordToS3` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 12 月 5 日 00:10 UTC
- 編集日時: 2020 年 12 月 5 日 00:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/IVSRecordToS3`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::AWSIVS_*/ivs/*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

KafkaConnectServiceRolePolicy

説明: このポリシーは、ユーザーに代わって AWS リソースを管理するアクセス許可を Kafka Connect に付与します。

KafkaConnectServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 9 月 7 日 13:12 UTC
- 編集日時: 2021 年 9 月 7 日 13:12 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/KafkaConnectServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

KafkaServiceRolePolicy

説明: Kafka の IAM サービスリンクロールポリシー。

KafkaServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 11 月 15 日 23:31 UTC
- 編集日時: 2025 年 11 月 10 日 23:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/KafkaServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:AttachNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DetachNetworkInterface",
        "ec2:DescribeVpcEndpoints",
        "acm-pca:GetCertificateAuthorityCertificate",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource" : "arn:*:ec2:*:*:subnet/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVpcEndpoints",
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource" : "arn:*:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AWSMSKManaged" : "true"
        },
        "StringLike" : {
          "ec2:ResourceTag/ClusterArn" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:PutResourcePolicy",
        "secretsmanager:DeleteResourcePolicy",
        "secretsmanager:DescribeSecret"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "secretsmanager:SecretId" : "arn:*:secretsmanager:*:*:secret:AmazonMSK_*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignIpv6Addresses",
        "ec2:UnassignIpv6Addresses",
```

```
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:*:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AWSMSKManaged" : "true"
        },
        "StringLike" : {
          "ec2:ResourceTag/ClusterArn" : "*"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

KeyspacesCDCServiceRolePolicy

説明: 変更データキャプチャに必要なアクセス許可を Amazon Keyspaces に付与します。

`KeyspacesCDCServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2025 年 6 月 21 日 00:22 UTC
- 編集日時: 2025 年 6 月 21 日 00:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/KeyspacesCDCServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "KeyspacesPutMetricDataPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Cassandra"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

KeyspacesReplicationServiceRolePolicy

説明: クロスリージョンデータレプリケーションのために Keyspaces が必要とするアクセス許可

KeyspacesReplicationServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 5 月 2 日 16:15 UTC
- 編集日時: 2024 年 11 月 15 日 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/KeyspacesReplicationServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "KeyspacesActionsNeededForSteadyStateReplication",
      "Effect" : "Allow",
      "Action" : [
        "cassandra:Select",
        "cassandra:Modify",
        "cassandra:Alter",
        "cassandra:ModifyMultiRegionResource",
        "cassandra:SelectMultiRegionResource",
        "cassandra:AlterMultiRegionResource",
        "application-autoscaling:RegisterScalableTarget",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
```

```
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CWDeleteAlarmPolicy",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:TargetTracking-*"
    },
    {
      "Sid" : "CWDescribeAlarmPolicy",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:*"
    },
    {
      "Sid" : "CWPutMetricAlarmPolicy",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:TargetTracking-*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "cloudwatch:AlarmActions" : [
            "arn:aws:autoscaling:*:*:scalingPolicy:*:resource/cassandra/keyspace/*/
table/*:policyName/*:createdBy/*"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する

- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

LakeFormationDataAccessServiceRolePolicy

説明: Lake Formation リソースへの一時的なデータアクセスを許可するポリシー

LakeFormationDataAccessServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 6 月 20 日 20:46 UTC
- 編集日時: 2024 年 2 月 6 日 18:37 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/LakeFormationDataAccessServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LakeFormationDataAccessServiceRolePolicy",
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

LexBotPolicy

説明: AWS Lex Bot ユースケースのポリシー

`LexBotPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 2 月 17 日 22:18 UTC
- 編集日時: 2019 年 11 月 13 日 22:29 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LexBotPolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "polly:SynthesizeSpeech"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "comprehend:DetectSentiment"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

LexChannelPolicy

説明: AWS Lex Channel ユースケースのポリシー

`LexChannelPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 2 月 17 日 23:23 UTC
- 編集日時: 2017 年 2 月 17 日 23:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LexChannelPolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "lex:PostText"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する

- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

LightsailExportAccess

説明: AWS Lightsail リソースをエクスポートするアクセス許可を付与するサービスにリンクされたロールポリシー

LightsailExportAccess は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 9 月 28 日 16:35 UTC
- 編集日時: 2022 年 1 月 15 日 01:45 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/LightsailExportAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

MediaConnectGatewayInstanceRolePolicy

説明: このポリシーは、MediaConnect ゲートウェイインスタンスを MediaConnect ゲートウェイに登録する許可を付与します。

`MediaConnectGatewayInstanceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `MediaConnectGatewayInstanceRolePolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 3 月 22 日 20:43 UTC
- 編集日時: 2023 年 3 月 22 日 20:43 UTC
- ARN: `arn:aws:iam::aws:policy/MediaConnectGatewayInstanceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MediaConnectGateway",
      "Effect" : "Allow",
      "Action" : [
        "mediaconnect:DiscoverGatewayPollEndpoint",
        "mediaconnect:PollGateway",
        "mediaconnect:SubmitGatewayStateChange"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

MediaPackageServiceRolePolicy

説明: MediaPackage が CloudWatch にログを発行することを許可

MediaPackageServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 9 月 18 日 17:45 UTC
- 編集日時: 2020 年 9 月 18 日 17:45 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/MediaPackageServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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/*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

MemoryDBServiceRolePolicy

説明: このポリシーは、MemoryDB がユーザーに代わって AWS リソースを管理することを許可します。

MemoryDBServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 8 月 17 日 22:34 UTC
- 編集日時: 2024 年 12 月 1 日 16:21 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/MemoryDBServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateMemoryDBTagsOnNetworkInterfaces",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonMemoryDBManaged"
          ]
        }
      }
    },
    {
      "Sid" : "CreateNetworkInterfaces",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
```

```
    {
      "Sid" : "DeleteMemoryDBTaggedNetworkInterfaces",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AmazonMemoryDBManaged" : "true"
        }
      }
    },
    {
      "Sid" : "DeleteNetworkInterfaces",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*"
    },
    {
      "Sid" : "DescribeEC2Resources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PutCloudWatchMetricData",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "cloudwatch:namespace" : "AWS/MemoryDB"
        }
      }
    },
    {
      "Sid" : "ReplicateMemoryDBMultiRegionClusterData",
      "Effect" : "Allow",
      "Action" : [
        "memorydb:ReplicateMultiRegionClusterData"
      ],
      "Resource" : "arn:aws:memorydb:*:*:cluster/*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

MigrationHubDMSAccessServiceRolePolicy

説明: Database Migration Service が Migration Hub を呼び出すために顧客のアカウントでロールを引き受けるためのポリシー

`MigrationHubDMSAccessServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 6 月 12 日 17:50 UTC
- 編集日時: 2019 年 10 月 7 日 17:57 UTC

- ARN: arn:aws:iam::aws:policy/aws-service-role/MigrationHubDMSAccessServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

MigrationHubServiceRolePolicy

説明: Migration Hub がユーザーに代わって Application Discovery Service を呼び出すことを許可

`MigrationHubServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 6 月 12 日 17:22 UTC
- 編集日時: 2020 年 8 月 6 日 18:08 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MigrationHubServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

MigrationHubSMSAccessServiceRolePolicy

説明: Server Migration Service が、Migration Hub を呼び出すために顧客アカウントでロールを引き受けるためのポリシー

`MigrationHubSMSAccessServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 6 月 12 日 18:30 UTC
- 編集日時: 2019 年 10 月 7 日 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MigrationHubSMSAccessServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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" : "*"
```

```
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

MonitronServiceRolePolicy

説明: 必要な顧客リソースへのアクセスを許可する AWS Monitron サービスにリンクされたロールのポリシー。

MonitronServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 5 月 2 日 19:22 UTC
- 編集日時: 2022 年 5 月 2 日 19:22 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/MonitronServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/monitron/*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

MultiPartyApprovalFullAccess

説明: マルチパーティー承認へのフルアクセスを提供します。このポリシーには、承認チームと ID ソースを管理するための AWS Organizations と AWS IAM Identity への関連するアクセス許可も含まれています。

`MultiPartyApprovalFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `MultiPartyApprovalFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 6 月 18 日 20:22 UTC

- 編集日時: 2025 年 9 月 8 日 17:04 UTC
- ARN: arn:aws:iam::aws:policy/MultiPartyApprovalFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MpaFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "mpa:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSOCreateApplication",
      "Effect" : "Allow",
      "Action" : [
        "sso:CreateApplication"
      ],
      "Resource" : [
        "arn:aws:sso:::instance/*",
        "arn:aws:sso::aws:applicationProvider/mpa"
```

```
      ]
    },
    {
      "Sid" : "SSOApplicationManagement",
      "Effect" : "Allow",
      "Action" : [
        "sso:DescribeApplication",
        "sso:PutApplicationAssignmentConfiguration",
        "sso:PutApplicationGrant",
        "sso:PutApplicationAuthenticationMethod",
        "sso:PutApplicationAccessScope",
        "sso:DeleteApplication"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "aws:CalledViaLast" : "mpa.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SSOManagementAccess",
      "Effect" : "Allow",
      "Action" : [
        "sso:DescribeInstance",
        "sso:DescribeRegisteredRegions",
        "sso:GetSharedSsoConfiguration",
        "sso-directory:DescribeUsers",
        "sso-directory:SearchUsers",
        "sso:ListInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:*:sso:::instance/*"
        },
```

```
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityStore",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
 "arn:*:identitystore::*:identitystore/*"
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

MultiPartyApprovalReadOnlyAccess

説明: マルチパーティー承認への読み取り専用アクセスを提供します。このポリシーには、承認チームと ID ソースに対する AWS Organizations と AWS IAM Identity への関連する読み取りアクセス許可も含まれています。

`MultiPartyApprovalReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに MultiPartyApprovalReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 6 月 18 日 20:07 UTC
- 編集日時: 2025 年 9 月 8 日 17:04 UTC
- ARN: arn:aws:iam::aws:policy/MultiPartyApprovalReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MpaReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "mpa:Get*",
        "mpa:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators",
        "organizations:DescribeOrganization"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSOManagementAccess",
      "Effect" : "Allow",
      "Action" : [
        "sso:DescribeInstance",
        "sso:ListInstances",
        "sso:DescribeRegisteredRegions",
        "sso:GetSharedSsoConfiguration",
        "sso-directory:DescribeUsers",
        "sso-directory:SearchUsers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:*:sso:::instance/*"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityStore",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
"arn:*:identitystore::*:identitystore/*"
        },
```

```
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

NeptuneConsoleFullAccess

説明: AWS マネジメントコンソールを使用して Amazon Neptune を管理するためのフルアクセスを提供します。このポリシーでは、アカウント内のすべての SNS トピックを公開するためのフルアクセス、Amazon EC2 インスタンスおよび VPC 設定を作成および編集する許可、Amazon KMS でキーを表示および一覧表示する許可、Amazon RDS へのフルアクセスも付与されることにご注意ください。詳細については、https://aws.amazon.com/neptune/faqs/ を参照してください。

`NeptuneConsoleFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `NeptuneConsoleFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 6 月 19 日 21:35 UTC
- 編集日時: 2023 年 11 月 30 日 07:32 UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneConsoleFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

NeptuneFullAccess

説明: Amazon Neptune へのフルアクセスを提供します。このポリシーでは、アカウント内のすべての SNS トピックに公開するためのフルアクセスおよび Amazon RDS へのフルアクセスも付与され

ることにご注意ください。詳細については、https://aws.amazon.com/neptune/faqs/ を参照してください。

NeptuneFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに NeptuneFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 5 月 30 日 19:17 UTC
- 編集日時: 2024 年 1 月 22 日 16:32 UTC
- ARN: arn:aws:iam::aws:policy/NeptuneFullAccess

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

NeptuneGraphReadOnlyAccess

説明: Amazon Neptune Analytics のすべてのリソースへの読み取り専用アクセスと、依存サービスへの読み取り専用アクセス許可を提供します。

`NeptuneGraphReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `NeptuneGraphReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 11 月 30 日 07:32 UTC
- 編集日時: 2023 年 11 月 30 日 07:32 UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneGraphReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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:*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

NeptuneReadOnlyAccess

説明: Amazon Neptune への読み取り専用アクセスを提供します。このポリシーでは、Amazon RDS リソースへのアクセスも付与されることにご注意ください。詳細については、https://aws.amazon.com/neptune/faqs/ を参照してください。

`NeptuneReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `NeptuneReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 5 月 30 日 19:16 UTC
- 編集日時: 2024 年 1 月 22 日 16:33 UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

NetworkAdministrator

説明: AWS ネットワークリソースのセットアップと設定に必要な AWS サービスとアクションへのフルアクセス許可を付与します。

NetworkAdministrator は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに NetworkAdministrator をアタッチできます。

ポリシーの詳細

- タイプ: ジョブ機能ポリシー
- 作成日時: 2016 年 11 月 10 日 17:31 UTC
- 編集日時: 2024 年 12 月 19 日 22:52 UTC
- ARN: arn:aws:iam::aws:policy/job-function/NetworkAdministrator

ポリシーのバージョン

ポリシーのバージョン: v13 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowDefaultNetworkAdminActions",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:Describe*",
        "cloudfront:ListDistributions",
```

```
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:PutMetricAlarm",
        "directconnect:*",
        "ec2:AcceptVpcEndpointConnections",
        "ec2:AllocateAddress",
        "ec2:AssignIpv6Addresses",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssociateAddress",
        "ec2:AssociateDhcpOptions",
        "ec2:AssociateRouteTable",
        "ec2:AssociateSubnetCidrBlock",
        "ec2:AssociateVpcCidrBlock",
        "ec2:AttachInternetGateway",
        "ec2:AttachNetworkInterface",
        "ec2:AttachVpnGateway",
        "ec2:CreateCarrierGateway",
        "ec2:CreateCustomerGateway",
        "ec2:CreateDefaultSubnet",
        "ec2:CreateDefaultVpc",
        "ec2:CreateDhcpOptions",
        "ec2:CreateEgressOnlyInternetGateway",
        "ec2:CreateFlowLogs",
        "ec2:CreateInternetGateway",
        "ec2:CreateNatGateway",
        "ec2:CreateNetworkAcl",
        "ec2:CreateNetworkAclEntry",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:CreatePlacementGroup",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateTags",
        "ec2:CreateVpc",
        "ec2:CreateVpcEndpoint",
        "ec2:CreateVpcEndpointConnectionNotification",
        "ec2:CreateVpcEndpointServiceConfiguration",
        "ec2:CreateVpnConnection",
        "ec2:CreateVpnConnectionRoute",
        "ec2:CreateVpnGateway",
        "ec2:DeleteCarrierGateway",
```

```
        "ec2:DeleteEgressOnlyInternetGateway",
        "ec2:DeleteFlowLogs",
        "ec2:DeleteNatGateway",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DeletePlacementGroup",
        "ec2:DeleteSubnet",
        "ec2:DeleteTags",
        "ec2:DeleteVpc",
        "ec2:DeleteVpcEndpointConnectionNotifications",
        "ec2:DeleteVpcEndpointServiceConfigurations",
        "ec2:DeleteVpcEndpoints",
        "ec2:DeleteVpnConnection",
        "ec2:DeleteVpnConnectionRoute",
        "ec2:DeleteVpnGateway",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCarrierGateways",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeIpv6Pools",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeMovingAddresses",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePlacementGroups",
        "ec2:DescribePrefixLists",
        "ec2:DescribePublicIpv4Pools",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupReferences",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeStaleSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
```

```
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeVpcClassicLinkDnsSupport",
        "ec2:DescribeVpcEndpointConnectionNotifications",
        "ec2:DescribeVpcEndpointConnections",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpointServicePermissions",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:DetachInternetGateway",
        "ec2:DetachNetworkInterface",
        "ec2:DetachVpnGateway",
        "ec2:DisableVgwRoutePropagation",
        "ec2:DisableVpcClassicLinkDnsSupport",
        "ec2:DisassociateAddress",
        "ec2:DisassociateRouteTable",
        "ec2:DisassociateSubnetCidrBlock",
        "ec2:DisassociateVpcCidrBlock",
        "ec2:EnableVgwRoutePropagation",
        "ec2:EnableVpcClassicLinkDnsSupport",
        "ec2:GetVpnConnectionDeviceSampleConfiguration",
        "ec2:GetVpnConnectionDeviceTypes",
        "ec2:GetVpnTunnelReplacementStatus",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifySecurityGroupRules",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:ModifyVpcEndpoint",
        "ec2:ModifyVpcEndpointConnectionNotification",
        "ec2:ModifyVpcEndpointServiceConfiguration",
        "ec2:ModifyVpcEndpointServicePermissions",
        "ec2:ModifyVpcPeeringConnectionOptions",
        "ec2:ModifyVpcTenancy",
        "ec2:ModifyVpnConnection",
        "ec2:ModifyVpnConnectionOptions",
        "ec2:ModifyVpnTunnelCertificate",
        "ec2:ModifyVpnTunnelOptions",
        "ec2:MoveAddressToVpc",
        "ec2:RejectVpcEndpointConnections",
        "ec2:ReleaseAddress",
```

```
        "ec2:ReplaceNetworkAclAssociation",
        "ec2:ReplaceNetworkAclEntry",
        "ec2:ReplaceRoute",
        "ec2:ReplaceRouteTableAssociation",
        "ec2:ReplaceVpnTunnel",
        "ec2:ResetNetworkInterfaceAttribute",
        "ec2:RestoreAddressToClassic",
        "ec2:UnassignIpv6Addresses",
        "ec2:UnassignPrivateIpAddresses",
        "ec2:UpdateSecurityGroupRuleDescriptionsEgress",
        "ec2:UpdateSecurityGroupRuleDescriptionsIngress",
        "elasticbeanstalk:Describe*",
        "elasticbeanstalk:List*",
        "elasticbeanstalk:RequestEnvironmentInfo",
        "elasticbeanstalk:RetrieveEnvironmentInfo",
        "elasticloadbalancing:*",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "route53:*",
        "route53domains:*",
        "sns:CreateTopic",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowVPCPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AcceptVpcPeeringConnection",
        "ec2:AssociateSecurityGroupVpc",
        "ec2:AttachClassicLinkVpc",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateVpcPeeringConnection",
        "ec2:DeleteCustomerGateway",
        "ec2:DeleteDhcpOptions",
        "ec2:DeleteInternetGateway",
        "ec2:DeleteNetworkAcl",
        "ec2:DeleteNetworkAclEntry",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
```

```
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteVolume",
        "ec2:DeleteVpcPeeringConnection",
        "ec2:DescribeSecurityGroupVpcAssociations",
        "ec2:DetachClassicLinkVpc",
        "ec2:DisableVpcClassicLink",
        "ec2:DisassociateSecurityGroupVpc",
        "ec2:EnableVpcClassicLink",
        "ec2:GetConsoleScreenshot",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:RejectVpcPeeringConnection",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowLocalGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLocalGatewayRoute",
        "ec2:CreateLocalGatewayRouteTableVpcAssociation",
        "ec2:DeleteLocalGatewayRoute",
        "ec2:DeleteLocalGatewayRouteTableVpcAssociation",
        "ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayVirtualInterfaceGroups",
        "ec2:DescribeLocalGatewayVirtualInterfaces",
        "ec2:DescribeLocalGateways",
        "ec2:SearchLocalGatewayRoutes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DiscoverBuckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:GetBucketWebsite",
        "s3:ListBucket"
      ],
```

```
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DiscoverFlowLogRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRoles",
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/flow-logs-*"
    },
    {
      "Sid" : "NetworkmanagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "networkmanager:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TransitGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AcceptTransitGatewayVpcAttachment",
        "ec2:AssociateTransitGatewayRouteTable",
        "ec2:CreateTransitGateway",
        "ec2:CreateTransitGatewayRoute",
        "ec2:CreateTransitGatewayRouteTable",
        "ec2:CreateTransitGatewayVpcAttachment",
        "ec2:DeleteTransitGateway",
        "ec2:DeleteTransitGatewayRoute",
        "ec2:DeleteTransitGatewayRouteTable",
        "ec2:DeleteTransitGatewayVpcAttachment",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DisableTransitGatewayRouteTablePropagation",
        "ec2:DisassociateTransitGatewayRouteTable",
        "ec2:EnableTransitGatewayRouteTablePropagation",
        "ec2:ExportTransitGatewayRoutes",
```

```
        "ec2:GetTransitGatewayAttachmentPropagations",
        "ec2:GetTransitGatewayRouteTableAssociations",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:ModifyTransitGateway",
        "ec2:ModifyTransitGatewayVpcAttachment",
        "ec2:RejectTransitGatewayVpcAttachment",
        "ec2:ReplaceTransitGatewayRoute",
        "ec2:SearchTransitGatewayRoutes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowTransitGatewaySLRCreation",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : [
            "transitgateway.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

NetworkSecurityDirectorServiceLinkedRolePolicy

説明: Shield AWS ネットワークセキュリティディレクターサービスにリンクされたロールが、指定された環境を評価するためのアクセス許可を提供します。

NetworkSecurityDirectorServiceLinkedRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2025 年 6 月 13 日 20:07 UTC
- 編集日時: 2025 年 11 月 10 日 19:49 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/NetworkSecurityDirectorServiceLinkedRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ResourceLevelPermissionNotSupported",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeManagedPrefixLists",
```

```
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:GetManagedPrefixListEntries",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "wafv2:ListWebACLs",
        "cloudfront:ListDistributions",
        "cloudfront:ListTagsForResource",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "cloudfront",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:GetDistribution"
      ],
      "Resource" : "arn:aws:cloudfront::*:distribution/*"
```

```
    },
    {
      "Sid" : "classicWaf",
      "Effect" : "Allow",
      "Action" : [
        "waf:ListWebACLs",
        "waf:GetWebACL"
      ],
      "Resource" : [
        "arn:aws:waf::*:webacl/*",
        "arn:aws:waf-regional:*:*:webacl/*"
      ]
    },
    {
      "Sid" : "wafv2",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:ListResourcesForWebACL",
        "wafv2:ListRuleGroups",
        "wafv2:ListAvailableManagedRuleGroups",
        "wafv2:GetRuleGroup",
        "wafv2:DescribeManagedRuleGroup",
        "wafv2:GetWebACL"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:global/rulegroup/*",
        "arn:aws:wafv2:*:*:regional/rulegroup/*",
        "arn:aws:wafv2:*:*:global/managedruleset/*",
        "arn:aws:wafv2:*:*:regional/managedruleset/*",
        "arn:aws:wafv2:*:*:global/webacl/*/*",
        "arn:aws:wafv2:*:*:regional/webacl/*/*",
        "arn:aws:apprunner:*:*:service/*",
        "arn:aws:cognito-idp:*:*:userpool/*",
        "arn:aws:ec2:*:*:verified-access-instance/*"
      ]
    },
    {
      "Sid" : "directconnect",
      "Effect" : "Allow",
      "Action" : [
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAssociations",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeVirtualGateways"
```

```
      ],
      "Resource" : [
        "arn:aws:directconnect::*:dx-gateway/*",
        "arn:aws:directconnect:*:*:dxcon/*",
        "arn:aws:directconnect:*:*:dxlag/*",
        "arn:aws:directconnect:*:*:dxvif/*"
      ]
    },
    {
      "Sid" : "ec2Get",
      "Effect" : "Allow",
      "Action" : [
        "ec2:SearchTransitGatewayRoutes"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:transit-gateway-route-table/*"
      ]
    },
    {
      "Sid" : "networkFirewall",
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:ListFirewalls",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListRuleGroups",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeRuleGroup"
      ],
      "Resource" : [
        "arn:aws:network-firewall:*:*:*/*"
      ]
    },
    {
      "Sid" : "apiGatewayGetAPI",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*",
```

```
        "arn:aws:apigateway:*::/tags/*",
        "arn:aws:apigateway:*::/vpclinks",
        "arn:aws:apigateway:*::/vpclinks/*"
      ]
    },
    {
      "Sid" : "AllowOrganizationsReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListChildren",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListRoots",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListTargetsForPolicy"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowOrganizationsAdmins",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "organizations:ServicePrincipal" : [
            "network-security-director.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowAccountInformationRead",
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
```

```
        "account:GetRegionOptStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowConfigRecorderList",
      "Effect" : "Allow",
      "Action" : [
        "config:ListConfigurationRecorders"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowConfigRecorderScopedAccess",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:PutServiceLinkedConfigurationRecorder",
        "config:DeleteServiceLinkedConfigurationRecorder"
      ],
      "Condition" : {
        "StringLikeIfExists" : {
          "config:ConfigurationRecorderServicePrincipal" : [
            "network-security-director.amazonaws.com"
          ]
        }
      },
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

NovaActServiceRolePolicy

説明: このポリシーにより、NovaAct は Nova Act エージェントを運用するために必要なリソースを作成および管理できます。

NovaActServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2025 年 11 月 26 日 16:19 UTC
- 編集日時: 2025 年 11 月 26 日 16:19 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/NovaActServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowPublishCloudWatchMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/NovaAct"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

OAMFullAccess

説明: CloudWatch オブザーバビリティ Access Manager へのフルアクセスを提供します

`OAMFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `OAMFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 11 月 27 日 13:38 UTC
- 編集日時: 2022 年 11 月 27 日 13:38 UTC
- ARN: `arn:aws:iam::aws:policy/OAMFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

OAMReadOnlyAccess

説明: CloudWatch オブザーバビリティ Access Manager への読み取り専用アクセスを提供します

`OAMReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `OAMReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 11 月 27 日 13:29 UTC
- 編集日時: 2022 年 11 月 27 日 13:29 UTC

- ARN: arn:aws:iam::aws:policy/OAMReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:Get*",
        "oam:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

OpensearchIngestionSelfManagedVpcePolicy

説明: Amazon OpenSearch Ingestion がネットワークリソースを記述し、サービスメトリクスを Cloudwatch に書き込むことを許可します

OpensearchIngestionSelfManagedVpcePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2024 年 6 月 10 日 19:59 UTC
- 編集日時: 2024 年 6 月 10 日 19:59 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/OpensearchIngestionSelfManagedVpcePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

PartnerCentralAccountManagementUserRoleAssociation

説明: パートナーセントラルユーザーの IAM ロールへの関連付け、および関連付け解除のためのアクセスを提供します。

PartnerCentralAccountManagementUserRoleAssociation は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに PartnerCentralAccountManagementUserRoleAssociation をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 11 月 10 日 02:03 UTC
- 編集日時: 2023 年 11 月 10 日 02:03 UTC

- ARN: `arn:aws:iam::aws:policy/PartnerCentralAccountManagementUserRoleAssociation`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

PowerUserAccess

説明: AWS サービスとリソースへのフルアクセスを提供しますが、ユーザーとグループの管理は許可しません。

PowerUserAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに PowerUserAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:39 UTC
- 編集日時: 2025 年 4 月 29 日 19:07 UTC
- ARN: arn:aws:iam::aws:policy/PowerUserAccess

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "NotAction" : [
        "iam:*",
        "organizations:*",
        "account:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
        "account:GetPrimaryEmail",
        "account:ListRegions",
        "iam:CreateServiceLinkedRole",
        "iam:DeleteServiceLinkedRole",
        "iam:ListRoles",
        "organizations:DescribeEffectivePolicy",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

QAppsServiceRolePolicy

説明: Amazon Q Apps が使用または管理する AWS のサービス および リソースにアクセス許可を付与します。

`QAppsServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2024 年 9 月 26 日 19:22 UTC
- 編集日時: 2024 年 9 月 26 日 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/QAppsServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "QAppsPutMetricDataPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/QApps"
        }
      }
    }
  ]
```

```
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

QBusinessQuicksightPluginPolicy

説明: QuickSight プラグイン用に QuickSight API を呼び出すアクセス許可を QBusiness に付与します。

`QBusinessQuicksightPluginPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `QBusinessQuicksightPluginPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 12 月 3 日 15:36 UTC
- 編集日時: 2024 年 12 月 3 日 15:36 UTC
- ARN: `arn:aws:iam::aws:policy/QBusinessQuicksightPluginPolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "QBusinessToQuickSightPredictQAResultsInvocation",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:PredictQAResults"
      ],
      "Resource" : [
        "arn:aws:quicksight:*:*:topic/*",
        "arn:aws:quicksight:*:*:dashboard/*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

QBusinessServiceRolePolicy

説明: Amazon Q が使用または管理する AWS のサービス およびリソースにアクセス許可を付与します

QBusinessServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー

- 作成日時: 2024 年 4 月 29 日 16:05 UTC
- 編集日時: 2024 年 4 月 29 日 16:05 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/QBusinessServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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}"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

QuickSightAccessForS3StorageManagementAnalyticsReadOnly

説明: QuickSight チームが、S3 ストレージ管理分析によって作成される顧客データにアクセスするために使用するポリシーです。

QuickSightAccessForS3StorageManagementAnalyticsReadOnly は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに QuickSightAccessForS3StorageManagementAnalyticsReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2017 年 6 月 12 日 18:18 UTC
- 編集日時: 2019 年 10 月 8 日 23:53 UTC
- ARN: arn:aws:iam::aws:policy/service-role/QuickSightAccessForS3StorageManagementAnalyticsReadOnly

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

RDSCloudHsmAuthorizationRole

説明: Amazon RDS サービスロールのデフォルトポリシー。

`RDSCloudHsmAuthorizationRole` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `RDSCloudHsmAuthorizationRole` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2019 年 9 月 26 日 22:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/RDSCloudHsmAuthorizationRole`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudhsm:CreateLunaClient",
        "cloudhsm:DeleteLunaClient",
        "cloudhsm:DescribeHapg",
        "cloudhsm:DescribeLunaClient",
        "cloudhsm:GetConfig",
        "cloudhsm:ModifyHapg",
        "cloudhsm:ModifyLunaClient"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

ReadOnlyAccess

説明: AWS サービスとリソースへの読み取り専用アクセスを提供します。

ReadOnlyAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに ReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:39 UTC
- 編集日時: 2025 年 12 月 16 日 13:04 UTC
- ARN: arn:aws:iam::aws:policy/ReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v137 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadOnlyActionsGroup1",
      "Effect" : "Allow",
      "Action" : [
        "a4b:Get*",
        "a4b:List*",
        "a4b:Search*",
        "access-analyzer:GetAccessPreview",
        "access-analyzer:GetAnalyzedResource",
        "access-analyzer:GetAnalyzer",
        "access-analyzer:GetArchiveRule",
        "access-analyzer:GetFinding",
        "access-analyzer:GetFindingsStatistics",
        "access-analyzer:GetGeneratedPolicy",
```

```
        "access-analyzer:ListAccessPreviewFindings",
        "access-analyzer:ListAccessPreviews",
        "access-analyzer:ListAnalyzedResources",
        "access-analyzer:ListAnalyzers",
        "access-analyzer:ListArchiveRules",
        "access-analyzer:ListFindings",
        "access-analyzer:ListPolicyGenerations",
        "access-analyzer:ListTagsForResource",
        "access-analyzer:ValidatePolicy",
        "account:GetAccountInformation",
        "account:GetAlternateContact",
        "account:GetContactInformation",
        "account:GetPrimaryEmail",
        "account:GetRegionOptStatus",
        "account:ListRegions",
        "acm-pca:Describe*",
        "acm-pca:Get*",
        "acm-pca:List*",
        "acm:Describe*",
        "acm:Get*",
        "acm:List*",
        "action-recommendations:ListRecommendedActions",
        "aiops:GetEphemeralInvestigationResults",
        "aiops:GetInvestigation",
        "aiops:GetInvestigationEvent",
        "aiops:GetInvestigationGroup",
        "aiops:GetInvestigationResource",
        "aiops:ListInvestigationEvents",
        "aiops:ListInvestigationGroups",
        "aiops:ListInvestigations",
        "aiops:ValidateInvestigationGroup",
        "aiops:GetFact",
        "aiops:GetFactVersions",
        "aiops:GetReport",
        "aiops:ListFacts",
        "airflow:ListEnvironments",
        "airflow:ListTagsForResource",
        "amplify:GetApp",
        "amplify:GetBackendEnvironment",
        "amplify:GetBranch",
        "amplify:GetDomainAssociation",
        "amplify:GetJob",
        "amplify:GetWebhook",
        "amplify:ListApps",
```

```
        "amplify:ListArtifacts",
        "amplify:ListBackendEnvironments",
        "amplify:ListBranches",
        "amplify:ListDomainAssociations",
        "amplify:ListJobs",
        "amplify:ListTagsForResource",
        "amplify:ListWebhooks",
        "aoss:BatchGetCollection",
        "aoss: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:GetExtension",
        "appconfig:GetHostedConfigurationVersion",
        "appconfig:ListApplications",
        "appconfig:ListConfigurationProfiles",
        "appconfig:ListDeploymentStrategies",
        "appconfig:ListDeployments",
        "appconfig:ListEnvironments",
        "appconfig:ListExtensions",
        "appconfig:ListHostedConfigurationVersions",
        "appconfig:ListTagsForResource",
        "appfabric:GetAppAuthorization",
        "appfabric:GetAppBundle",
        "appfabric:GetIngestion",
        "appfabric:GetIngestionDestination",
        "appfabric:ListAppAuthorizations",
```

```
        "appfabric:ListAppBundles",
        "appfabric:ListIngestionDestinations",
        "appfabric:ListIngestions",
        "appfabric:ListTagsForResource",
        "appflow:DescribeConnector",
        "appflow:DescribeConnectorEntity",
        "appflow:DescribeConnectorFields",
        "appflow:DescribeConnectorProfiles",
        "appflow:DescribeConnectors",
        "appflow:DescribeFlow",
        "appflow:DescribeFlowExecution",
        "appflow:DescribeFlowExecutionRecords",
        "appflow:DescribeFlows",
        "appflow:ListConnectorEntities",
        "appflow:ListConnectorFields",
        "appflow:ListConnectors",
        "appflow:ListFlows",
        "appflow:ListTagsForResource",
        "application-autoscaling:Describe*",
        "application-autoscaling:GetPredictiveScalingForecast",
        "application-autoscaling:ListTagsForResource",
        "application-signals:BatchGetServiceLevelObjectiveBudgetReport",
        "application-signals:GetService",
        "application-signals:GetServiceLevelObjective",
        "application-signals:ListObservedEntities",
        "application-signals:ListServiceDependencies",
        "application-signals:ListServiceDependents",
        "application-signals:ListServiceLevelObjectives",
        "application-signals:ListServiceOperations",
        "application-signals:ListServices",
        "application-signals:ListTagsForResource",
        "application-signals:ListServiceStates",
        "application-signals:ListAuditFindings",
        "application-signals:ListGroupingAttributeDefinitions",
        "application-signals:ListServiceLevelObjectiveExclusionWindows",
        "application-signals:ListEntityEvents",
        "applicationinsights:Describe*",
        "applicationinsights:List*",
        "appmesh:Describe*",
        "appmesh:List*",
        "apprunner:DescribeAutoScalingConfiguration",
        "apprunner:DescribeCustomDomains",
        "apprunner:DescribeObservabilityConfiguration",
        "apprunner:DescribeService",
```

```
        "apprunner:DescribeVpcConnector",
        "apprunner:DescribeVpcIngressConnection",
        "apprunner:DescribeWebAclForService",
        "apprunner:ListAssociatedServicesForWebAcl",
        "apprunner:ListAutoScalingConfigurations",
        "apprunner:ListConnections",
        "apprunner:ListObservabilityConfigurations",
        "apprunner:ListOperations",
        "apprunner:ListServices",
        "apprunner:ListServicesForAutoScalingConfiguration",
        "apprunner:ListTagsForResource",
        "apprunner:ListVpcConnectors",
        "apprunner:ListVpcIngressConnections",
        "appstream:Describe*",
        "appstream:List*",
        "appstudio:GetAccountStatus",
        "appstudio:GetEnablementJobStatus",
        "appsync:Get*",
        "appsync:List*",
        "apptest:GetTestCase",
        "apptest:GetTestConfiguration",
        "apptest:GetTestRunStep",
        "apptest:GetTestSuite",
        "apptest:ListTagsForResource",
        "apptest:ListTestCases",
        "apptest:ListTestConfigurations",
        "apptest:ListTestRunSteps",
        "apptest:ListTestRunTestCases",
        "apptest:ListTestRuns",
        "apptest:ListTestSuites",
        "aps:DescribeAlertManagerDefinition",
        "aps:DescribeLoggingConfiguration",
        "aps:DescribeRuleGroupsNamespace",
        "aps:DescribeScraper",
        "aps:DescribeWorkspace",
        "aps:GetAlertManagerSilence",
        "aps:GetAlertManagerStatus",
        "aps:GetDefaultScraperConfiguration",
        "aps:GetLabels",
        "aps:GetMetricMetadata",
        "aps:GetSeries",
        "aps:ListAlertManagerAlertGroups",
        "aps:ListAlertManagerAlerts",
        "aps:ListAlertManagerReceivers",
```

```
        "aps:ListAlertManagerSilences",
        "aps:ListAlerts",
        "aps:ListRuleGroupsNamespaces",
        "aps:ListRules",
        "aps:ListScrapers",
        "aps:ListTagsForResource",
        "aps:ListWorkspaces",
        "aps:QueryMetrics",
        "arc-region-switch:GetPlan",
        "arc-region-switch:GetPlanEvaluationStatus",
        "arc-region-switch:GetPlanExecution",
        "arc-region-switch:GetPlanInRegion",
        "arc-region-switch:ListPlanExecutionEvents",
        "arc-region-switch:ListPlanExecutions",
        "arc-region-switch:ListPlans",
        "arc-region-switch:ListPlansInRegion",
        "arc-region-switch:ListRoute53HealthChecks",
        "arc-region-switch:ListTagsForResource",
        "arc-zonal-shift:GetAutoshiftObserverNotificationStatus",
        "arc-zonal-shift:GetManagedResource",
        "arc-zonal-shift:ListAutoshifts",
        "arc-zonal-shift:ListManagedResources",
        "arc-zonal-shift:ListZonalShifts",
        "artifact:GetCustomerAgreement",
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements",
        "artifact:ListReports",
        "athena:Batch*",
        "athena:Get*",
        "athena:List*",
        "auditmanager:GetAccountStatus",
        "auditmanager:GetAssessment",
        "auditmanager:GetAssessmentFramework",
        "auditmanager:GetAssessmentReportUrl",
        "auditmanager:GetChangeLogs",
        "auditmanager:GetControl",
        "auditmanager:GetDelegations",
        "auditmanager:GetEvidence",
        "auditmanager:GetEvidenceByEvidenceFolder",
        "auditmanager:GetEvidenceFolder",
        "auditmanager:GetEvidenceFoldersByAssessment",
```

```
        "auditmanager:GetEvidenceFoldersByAssessmentControl",
        "auditmanager:GetOrganizationAdminAccount",
        "auditmanager:GetServicesInScope",
        "auditmanager:GetSettings",
        "auditmanager:ListAssessmentFrameworks",
        "auditmanager:ListAssessmentReports",
        "auditmanager:ListAssessments",
        "auditmanager:ListControls",
        "auditmanager:ListKeywordsForDataSource",
        "auditmanager:ListNotifications",
        "auditmanager:ListTagsForResource",
        "auditmanager:ValidateAssessmentReportIntegrity",
        "autoscaling-plans:Describe*",
        "autoscaling-plans:GetScalingPlanResourceForecastData",
        "autoscaling:Describe*",
        "autoscaling:GetPredictiveScalingForecast",
        "aws-portal:View*",
        "backup-gateway:GetBandwidthRateLimitSchedule",
        "backup-gateway:GetGateway",
        "backup-gateway:GetHypervisor",
        "backup-gateway:GetHypervisorPropertyMappings",
        "backup-gateway:GetVirtualMachine",
        "backup-gateway:ListGateways",
        "backup-gateway:ListHypervisors",
        "backup-gateway:ListTagsForResource",
        "backup-gateway:ListVirtualMachines",
        "backup:Describe*",
        "backup:Get*",
        "backup:List*",
        "batch:Describe*",
        "batch:List*",
        "bedrock-agentcore:GetAgentRuntime",
        "bedrock-agentcore:GetAgentRuntimeEndpoint",
        "bedrock-agentcore:GetApiKeyCredentialProvider",
        "bedrock-agentcore:GetBrowser",
        "bedrock-agentcore:GetBrowserSession",
        "bedrock-agentcore:GetCodeInterpreter",
        "bedrock-agentcore:GetCodeInterpreterSession",
        "bedrock-agentcore:GetEvent",
        "bedrock-agentcore:GetGateway",
        "bedrock-agentcore:GetGatewayTarget",
        "bedrock-agentcore:GetMemory",
        "bedrock-agentcore:GetMemoryRecord",
        "bedrock-agentcore:GetOauth2CredentialProvider",
```

```
        "bedrock-agentcore:GetTokenVault",
        "bedrock-agentcore:GetWorkloadIdentity",
        "bedrock-agentcore:ListAgentRuntimeEndpoints",
        "bedrock-agentcore:ListAgentRuntimes",
        "bedrock-agentcore:ListAgentRuntimeVersions",
        "bedrock-agentcore:ListApiKeyCredentialProviders",
        "bedrock-agentcore:ListBrowsers",
        "bedrock-agentcore:ListBrowserSessions",
        "bedrock-agentcore:ListCodeInterpreters",
        "bedrock-agentcore:ListCodeInterpreterSessions",
        "bedrock-agentcore:ListEvents",
        "bedrock-agentcore:ListGateways",
        "bedrock-agentcore:ListGatewayTargets",
        "bedrock-agentcore:ListMemories",
        "bedrock-agentcore:ListMemoryRecords",
        "bedrock-agentcore:ListOauth2CredentialProviders",
        "bedrock-agentcore:ListWorkloadIdentities",
        "bedrock-agentcore:RetrieveMemoryRecords",
        "bedrock:GetAgent",
        "bedrock:GetAgentActionGroup",
        "bedrock:GetAgentAlias",
        "bedrock:GetAgentCollaborator",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:GetAgentVersion",
        "bedrock:GetCustomModel",
        "bedrock:GetDataSource",
        "bedrock:GetEvaluationJob",
        "bedrock:GetFlow",
        "bedrock:GetFlowAlias",
        "bedrock:GetFlowVersion",
        "bedrock:GetFoundationModel",
        "bedrock:GetFoundationModelAvailability",
        "bedrock:GetGuardrail",
        "bedrock:GetInferenceProfile",
        "bedrock:GetIngestionJob",
        "bedrock:GetKnowledgeBase",
        "bedrock:GetModelCustomizationJob",
        "bedrock:GetModelInvocationJob",
        "bedrock:GetModelInvocationLoggingConfiguration",
        "bedrock:GetPrompt",
        "bedrock:GetProvisionedModelThroughput",
        "bedrock:GetUseCaseForModelAccess",
        "bedrock:ListAgentActionGroups",
        "bedrock:ListAgentAliases",
```

```
        "bedrock:ListAgentCollaborators",
        "bedrock:ListAgentKnowledgeBases",
        "bedrock:ListAgentVersions",
        "bedrock:ListAgents",
        "bedrock:ListCustomModels",
        "bedrock:ListDataSources",
        "bedrock:ListEvaluationJobs",
        "bedrock:ListFlowAliases",
        "bedrock:ListFlowVersions",
        "bedrock:ListFlows",
        "bedrock:ListFoundationModelAgreementOffers",
        "bedrock:ListFoundationModels",
        "bedrock:ListGuardrails",
        "bedrock:ListInferenceProfiles",
        "bedrock:ListIngestionJobs",
        "bedrock:ListKnowledgeBases",
        "bedrock:ListModelCustomizationJobs",
        "bedrock:ListModelInvocationJobs",
        "bedrock:ListPrompts",
        "bedrock:ListProvisionedModelThroughputs",
        "billing:GetBillingData",
        "billing:GetBillingDetails",
        "billing:GetBillingNotifications",
        "billing:GetBillingPreferences",
        "billing:GetBillingView",
        "billing:GetContractInformation",
        "billing:GetCredits",
        "billing:GetIAMAccessPreference",
        "billing:GetResourcePolicy",
        "billing:GetSellerOfRecord",
        "billing:ListBillingViews",
        "billing:ListSourceViewsForBillingView",
        "billing:ListTagsForResource",
        "billingconductor:GetBillingGroupCostReport",
        "billingconductor:ListAccountAssociations",
        "billingconductor:ListBillingGroupCostReports",
        "billingconductor:ListBillingGroups",
        "billingconductor:ListCustomLineItemVersions",
        "billingconductor:ListCustomLineItems",
        "billingconductor:ListPricingPlans",
        "billingconductor:ListPricingPlansAssociatedWithPricingRule",
        "billingconductor:ListPricingRules",
        "billingconductor:ListPricingRulesAssociatedToPricingPlan",
        "billingconductor:ListResourcesAssociatedToCustomLineItem",
```

```
        "billingconductor:ListTagsForResource",
        "braket:GetDevice",
        "braket:GetJob",
        "braket:GetQuantumTask",
        "braket:SearchDevices",
        "braket:SearchJobs",
        "braket:SearchQuantumTasks",
        "budgets:Describe*",
        "budgets:ListTagsForResource",
        "budgets:View*",
        "cassandra:Select",
        "ce:DescribeCostCategoryDefinition",
        "ce:DescribeNotificationSubscription",
        "ce:DescribeReport",
        "ce:GetAnomalies",
        "ce:GetAnomalyMonitors",
        "ce:GetAnomalySubscriptions",
        "ce:GetApproximateUsageRecords",
        "ce:GetCommitmentPurchaseAnalysis",
        "ce:GetCostAndUsage",
        "ce:GetCostAndUsageComparisons",
        "ce:GetCostAndUsageWithResources",
        "ce:GetCostCategories",
        "ce:GetCostComparisonDrivers",
        "ce:GetCostForecast",
        "ce:GetDimensionValues",
        "ce:GetPreferences",
        "ce:GetReservationCoverage",
        "ce:GetReservationPurchaseRecommendation",
        "ce:GetReservationUtilization",
        "ce:GetRightsizingRecommendation",
        "ce:GetSavingsPlanPurchaseRecommendationDetails",
        "ce:GetSavingsPlansCoverage",
        "ce:GetSavingsPlansPurchaseRecommendation",
        "ce:GetSavingsPlansUtilization",
        "ce:GetSavingsPlansUtilizationDetails",
        "ce:GetTags",
        "ce:GetUsageForecast",
        "ce:ListCommitmentPurchaseAnalyses",
        "ce:ListCostAllocationTagBackfillHistory",
        "ce:ListCostAllocationTags",
        "ce:ListCostCategoryDefinitions",
        "ce:ListSavingsPlansPurchaseRecommendationGeneration",
        "ce:ListTagsForResource",
```

```
        "chatbot:Describe*",
        "chatbot:Get*",
        "chatbot:List*",
        "chime:Get*",
        "chime:List*",
        "chime:Retrieve*",
        "chime:Search*",
        "chime:Validate*",
        "cleanrooms-ml:GetAudienceGenerationJob",
        "cleanrooms-ml:GetAudienceModel",
        "cleanrooms-ml:GetConfiguredAudienceModel",
        "cleanrooms-ml:GetConfiguredAudienceModelPolicy",
        "cleanrooms-ml:GetTrainingDataset",
        "cleanrooms-ml:ListAudienceExportJobs",
        "cleanrooms-ml:ListAudienceGenerationJobs",
        "cleanrooms-ml:ListAudienceModels",
        "cleanrooms-ml:ListConfiguredAudienceModels",
        "cleanrooms-ml:ListTagsForResource",
        "cleanrooms-ml:ListTrainingDatasets",
        "cleanrooms:BatchGetCollaborationAnalysisTemplate",
        "cleanrooms:BatchGetSchema",
        "cleanrooms:BatchGetSchemaAnalysisRule",
        "cleanrooms:GetAnalysisTemplate",
        "cleanrooms:GetCollaboration",
        "cleanrooms:GetCollaborationAnalysisTemplate",
        "cleanrooms:GetCollaborationConfiguredAudienceModelAssociation",
        "cleanrooms:GetCollaborationIdNamespaceAssociation",
        "cleanrooms:GetCollaborationPrivacyBudgetTemplate",
        "cleanrooms:GetConfiguredAudienceModelAssociation",
        "cleanrooms:GetConfiguredTable",
        "cleanrooms:GetConfiguredTableAnalysisRule",
        "cleanrooms:GetConfiguredTableAssociation",
        "cleanrooms:GetConfiguredTableAssociationAnalysisRule",
        "cleanrooms:GetIdMappingTable",
        "cleanrooms:GetIdNamespaceAssociation",
        "cleanrooms:GetMembership",
        "cleanrooms:GetPrivacyBudgetTemplate",
        "cleanrooms:GetProtectedQuery",
        "cleanrooms:GetSchema",
        "cleanrooms:GetSchemaAnalysisRule",
        "cleanrooms:ListAnalysisTemplates",
        "cleanrooms:ListCollaborationAnalysisTemplates",
        "cleanrooms:ListCollaborationConfiguredAudienceModelAssociations",
        "cleanrooms:ListCollaborationIdNamespaceAssociations",
```

```
        "cleanrooms:ListCollaborationPrivacyBudgetTemplates",
        "cleanrooms:ListCollaborationPrivacyBudgets",
        "cleanrooms:ListCollaborations",
        "cleanrooms:ListConfiguredAudienceModelAssociations",
        "cleanrooms:ListConfiguredTableAssociations",
        "cleanrooms:ListConfiguredTables",
        "cleanrooms:ListIdMappingTables",
        "cleanrooms:ListIdNamespaceAssociations",
        "cleanrooms:ListMembers",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListPrivacyBudgetTemplates",
        "cleanrooms:ListPrivacyBudgets",
        "cleanrooms:ListProtectedQueries",
        "cleanrooms:ListSchemas",
        "cleanrooms:ListTagsForResource",
        "cleanrooms:PreviewPrivacyImpact",
        "cleanrooms:GetCollaborationChangeRequest",
        "cleanrooms:GetProtectedJob",
        "cleanrooms:ListCollaborationChangeRequests",
        "cleanrooms:ListProtectedJobs",
        "cloud9:Describe*",
        "cloud9:List*",
        "clouddirectory:BatchRead",
        "clouddirectory:Get*",
        "clouddirectory:List*",
        "clouddirectory:LookupPolicy",
        "cloudformation:Describe*",
        "cloudformation:Detect*",
        "cloudformation:Estimate*",
        "cloudformation:Get*",
        "cloudformation:List*",
        "cloudformation:ValidateTemplate",
        "cloudfront-keyvaluestore:Describe*",
        "cloudfront-keyvaluestore:Get*",
        "cloudfront-keyvaluestore:List*",
        "cloudfront:Describe*",
        "cloudfront:Get*",
        "cloudfront:List*",
        "cloudhsm:Describe*",
        "cloudhsm:GetResourcePolicy",
        "cloudhsm:List*",
        "cloudsearch:Describe*",
        "cloudsearch:List*",
        "cloudtrail:Describe*",
```

```
        "cloudtrail:Get*",
        "cloudtrail:List*",
        "cloudtrail:LookupEvents",
        "cloudwatch:Describe*",
        "cloudwatch:GenerateQuery",
        "cloudwatch:GenerateQueryResultsSummary",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "codeartifact:DescribeDomain",
        "codeartifact:DescribePackage",
        "codeartifact:DescribePackageVersion",
        "codeartifact:DescribeRepository",
        "codeartifact:GetAuthorizationToken",
        "codeartifact:GetDomainPermissionsPolicy",
        "codeartifact:GetPackageVersionAsset",
        "codeartifact:GetPackageVersionReadme",
        "codeartifact:GetRepositoryEndpoint",
        "codeartifact:GetRepositoryPermissionsPolicy",
        "codeartifact:ListDomains",
        "codeartifact:ListPackageVersionAssets",
        "codeartifact:ListPackageVersionDependencies",
        "codeartifact:ListPackageVersions",
        "codeartifact:ListPackages",
        "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:ListTargets",
        "codestar-notifications:describeNotificationRule",
        "codestar-notifications:listEventTypes",
        "codestar-notifications:listNotificationRules",
        "codestar-notifications:listTagsForResource",
        "codestar:Describe*",
        "codestar:Get*",
        "codestar:List*",
        "codestar:Verify*",
        "codewhisperer:ListProfiles",
        "cognito-identity:Describe*",
        "cognito-identity:GetCredentialsForIdentity",
        "cognito-identity:GetIdentityPoolAnalytics",
        "cognito-identity:GetIdentityPoolDailyAnalytics",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:GetIdentityProviderDailyAnalytics",
        "cognito-identity:GetOpenIdToken",
        "cognito-identity:GetOpenIdTokenForDeveloperIdentity",
        "cognito-identity:List*",
        "cognito-identity:Lookup*",
        "cognito-idp:AdminGet*",
        "cognito-idp:AdminList*",
        "cognito-idp:Describe*",
```

```
        "cognito-idp:Get*",
        "cognito-idp:List*",
        "cognito-sync:Describe*",
        "cognito-sync:Get*",
        "cognito-sync:List*",
        "cognito-sync:QueryRecords",
        "comprehend:BatchDetect*",
        "comprehend:Classify*",
        "comprehend:Contains*",
        "comprehend:Describe*",
        "comprehend:Detect*",
        "comprehend:List*",
        "compute-optimizer:DescribeRecommendationExportJobs",
        "compute-optimizer:GetAutoScalingGroupRecommendations",
        "compute-optimizer:GetEBSVolumeRecommendations",
        "compute-optimizer:GetEC2InstanceRecommendations",
        "compute-optimizer:GetEC2RecommendationProjectedMetrics",
        "compute-optimizer:GetECSServiceRecommendationProjectedMetrics",
        "compute-optimizer:GetECSServiceRecommendations",
        "compute-optimizer:GetEffectiveRecommendationPreferences",
        "compute-optimizer:GetEnrollmentStatus",
        "compute-optimizer:GetEnrollmentStatusesForOrganization",
        "compute-optimizer:GetIdleRecommendations",
        "compute-optimizer:GetLambdaFunctionRecommendations",
        "compute-optimizer:GetLicenseRecommendations",
        "compute-optimizer:GetRDSDatabaseRecommendationProjectedMetrics",
        "compute-optimizer:GetRDSDatabaseRecommendations",
        "compute-optimizer:GetRecommendationPreferences",
        "compute-optimizer:GetRecommendationSummaries",
        "config:BatchGetAggregateResourceConfig",
        "config:BatchGetResourceConfig",
        "config:Deliver*",
        "config:Describe*",
        "config:Get*",
        "config:List*",
        "config:SelectAggregateResourceConfig",
        "config:SelectResourceConfig",
        "connect:Describe*",
        "connect:GetContactAttributes",
        "connect:GetCurrentMetricData",
        "connect:GetCurrentUserData",
        "connect:GetFederationToken",
        "connect:GetMetricData",
        "connect:GetMetricDataV2",
```

```
            "connect:GetTaskTemplate",
            "connect:GetTrafficDistribution",
            "connect:List*",
            "consoleapp:GetDeviceIdentity",
            "consoleapp:ListDeviceIdentities",
            "consolidatedbilling:GetAccountBillingRole",
            "consolidatedbilling:ListLinkedAccounts",
            "controlcatalog:GetControl",
            "controlcatalog:ListCommonControls",
            "controlcatalog:ListControlMappings",
            "controlcatalog:ListControls",
            "controlcatalog:ListDomains",
            "controlcatalog:ListObjectives",
            "cost-optimization-hub:GetPreferences",
            "cost-optimization-hub:GetRecommendation",
            "cost-optimization-hub:ListEnrollmentStatuses",
            "cost-optimization-hub:ListRecommendationSummaries",
            "cost-optimization-hub:ListRecommendations",
            "cost-optimization-hub:ListEfficiencyMetrics",
            "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:ListRecipeVersions",
            "databrew:ListRecipes",
            "databrew:ListRulesets",
            "databrew:ListSchedules",
            "databrew:ListTagsForResource",
            "dataexchange:Get*",
            "dataexchange:List*",
            "datapipeline:Describe*",
            "datapipeline:EvaluateExpression",
```

```
        "datapipeline:Get*",
        "datapipeline:List*",
        "datapipeline:QueryObjects",
        "datapipeline:Validate*",
        "datasync:Describe*",
        "datasync:List*",
        "datazone:GetAsset",
        "datazone:GetAssetType",
        "datazone:GetDataProduct",
        "datazone:GetDataSource",
        "datazone:GetDataSourceRun",
        "datazone:GetDomain",
        "datazone:GetDomainSharingPolicy",
        "datazone:GetDomainUnit",
        "datazone:GetEnvironment",
        "datazone:GetEnvironmentAction",
        "datazone:GetEnvironmentBlueprint",
        "datazone:GetEnvironmentBlueprintConfiguration",
        "datazone:GetEnvironmentProfile",
        "datazone:GetFormType",
        "datazone:GetGlossary",
        "datazone:GetGlossaryTerm",
        "datazone:GetGroupProfile",
        "datazone:GetLineageNode",
        "datazone:GetListing",
        "datazone:GetMetadataGenerationRun",
        "datazone:GetProject",
        "datazone:GetProjectProfile",
        "datazone:GetSubscription",
        "datazone:GetSubscriptionEligibility",
        "datazone:GetSubscriptionGrant",
        "datazone:GetSubscriptionRequestDetails",
        "datazone:GetSubscriptionTarget",
        "datazone:GetTimeSeriesDataPoint",
        "datazone:GetUserProfile",
        "datazone:ListAccountEnvironments",
        "datazone:ListAssetRevisions",
        "datazone:ListDataProductRevisions",
        "datazone:ListDataSourceRunActivities",
        "datazone:ListDataSourceRuns",
        "datazone:ListDataSources",
        "datazone:ListDomainUnitsForParent",
        "datazone:ListDomains",
        "datazone:ListEntityOwners",
```

```
        "datazone:ListEnvironmentActions",
        "datazone:ListEnvironmentBlueprintConfigurationSummaries",
        "datazone:ListEnvironmentBlueprintConfigurations",
        "datazone:ListEnvironmentBlueprints",
        "datazone:ListEnvironmentProfiles",
        "datazone:ListEnvironments",
        "datazone:ListGroupsForUser",
        "datazone:ListLineageNodeHistory",
        "datazone:ListNotifications",
        "datazone:ListPolicyGrants",
        "datazone:ListProjectMemberships",
        "datazone:ListProjectProfiles",
        "datazone:ListProjects",
        "datazone:ListSubscriptionGrants",
        "datazone:ListSubscriptionRequests",
        "datazone:ListSubscriptionTargets",
        "datazone:ListSubscriptions",
        "datazone:ListTagsForResource",
        "datazone:ListTimeSeriesDataPoints",
        "datazone:Search",
        "datazone:SearchGroupProfiles",
        "datazone:SearchListings",
        "datazone:SearchTypes",
        "datazone:SearchUserProfiles",
        "dax:BatchGetItem",
        "dax:Describe*",
        "dax:GetItem",
        "dax:ListTags",
        "dax:Query",
        "dax:Scan",
        "deadline:BatchGetJobEntity",
        "deadline:GetApplicationVersion",
        "deadline:GetBudget",
        "deadline:GetFarm",
        "deadline:GetFleet",
        "deadline:GetJob",
        "deadline:GetLicenseEndpoint",
        "deadline:GetMonitor",
        "deadline:GetQueue",
        "deadline:GetQueueEnvironment",
        "deadline:GetQueueFleetAssociation",
        "deadline:GetSession",
        "deadline:GetSessionAction",
        "deadline:GetSessionsStatisticsAggregation",
```

```
        "deadline:GetStep",
        "deadline:GetStorageProfile",
        "deadline:GetStorageProfileForQueue",
        "deadline:GetTask",
        "deadline:GetWorker",
        "deadline:ListAvailableMeteredProducts",
        "deadline:ListBudgets",
        "deadline:ListFarmMembers",
        "deadline:ListFarms",
        "deadline:ListFleetMembers",
        "deadline:ListFleets",
        "deadline:ListJobMembers",
        "deadline:ListJobParameterDefinitions",
        "deadline:ListJobs",
        "deadline:ListLicenseEndpoints",
        "deadline:ListMeteredProducts",
        "deadline:ListMonitors",
        "deadline:ListQueueEnvironments",
        "deadline:ListQueueFleetAssociations",
        "deadline:ListQueueMembers",
        "deadline:ListQueues",
        "deadline:ListSessionActions",
        "deadline:ListSessions",
        "deadline:ListSessionsForWorker",
        "deadline:ListStepConsumers",
        "deadline:ListStepDependencies",
        "deadline:ListSteps",
        "deadline:ListStorageProfiles",
        "deadline:ListStorageProfilesForQueue",
        "deadline:ListTagsForResource",
        "deadline:ListTasks",
        "deadline:ListWorkers",
        "deadline:SearchJobs",
        "deadline:SearchSteps",
        "deadline:SearchTasks",
        "deadline:SearchWorkers",
        "deepcomposer:GetComposition",
        "deepcomposer:GetModel",
        "deepcomposer:GetSampleModel",
        "deepcomposer:ListCompositions",
        "deepcomposer:ListModels",
        "deepcomposer:ListSampleModels",
        "deepcomposer:ListTrainingTopics",
        "detective:BatchGetGraphMemberDatasources",
```

```
        "detective:BatchGetMembershipDatasources",
        "detective:Get*",
        "detective:List*",
        "detective:SearchGraph",
        "devicefarm:Get*",
        "devicefarm:List*",
        "devops-guru:DescribeAccountHealth",
        "devops-guru:DescribeAccountOverview",
        "devops-guru:DescribeAnomaly",
        "devops-guru:DescribeEventSourcesConfig",
        "devops-guru:DescribeFeedback",
        "devops-guru:DescribeInsight",
        "devops-guru:DescribeOrganizationHealth",
        "devops-guru:DescribeOrganizationOverview",
        "devops-guru:DescribeOrganizationResourceCollectionHealth",
        "devops-guru:DescribeResourceCollectionHealth",
        "devops-guru:DescribeServiceIntegration",
        "devops-guru:GetCostEstimation",
        "devops-guru:GetResourceCollection",
        "devops-guru:ListAnomaliesForInsight",
        "devops-guru:ListAnomalousLogGroups",
        "devops-guru:ListEvents",
        "devops-guru:ListInsights",
        "devops-guru:ListMonitoredResources",
        "devops-guru:ListNotificationChannels",
        "devops-guru:ListOrganizationInsights",
        "devops-guru:ListRecommendations",
        "devops-guru:SearchInsights",
        "devops-guru:StartCostEstimation",
        "directconnect:Describe*",
        "discovery:Describe*",
        "discovery:Get*",
        "discovery:List*",
        "dlm:Get*",
        "dms:Describe*",
        "dms:List*",
        "dms:Test*",
        "docdb-elastic:ListClusters",
        "docdb-elastic:ListClusterSnapshots",
        "docdb-elastic:ListPendingMaintenanceActions",
        "docdb-elastic:ListTagsForResource",
        "drs:DescribeJobLogItems",
        "drs:DescribeJobs",
        "drs:DescribeLaunchConfigurationTemplates",
```

```
        "drs:DescribeRecoveryInstances",
        "drs:DescribeRecoverySnapshots",
        "drs:DescribeReplicationConfigurationTemplates",
        "drs:DescribeSourceNetworks",
        "drs:DescribeSourceServers",
        "drs:GetFailbackReplicationConfiguration",
        "drs:GetLaunchConfiguration",
        "drs:GetReplicationConfiguration",
        "drs:ListExtensibleSourceServers",
        "drs:ListLaunchActions",
        "drs:ListStagingAccounts",
        "drs:ListTagsForResource",
        "ds:Check*",
        "ds:Describe*",
        "ds:Get*",
        "ds:List*",
        "ds:Verify*",
        "dsql:GetCluster",
        "dsql:GetVpcEndpointServiceName",
        "dsql:ListClusters",
        "dsql:ListTagsForResource",
        "dynamodb:BatchGet*",
        "dynamodb:Describe*",
        "dynamodb:Get*",
        "dynamodb:List*",
        "dynamodb:PartiQLSelect",
        "dynamodb:Query",
        "dynamodb:Scan",
        "ec2:Describe*",
        "ec2:DescribeInstanceImageMetadata",
        "ec2:Get*",
        "ec2:ListImagesInRecycleBin",
        "ec2:ListSnapshotsInRecycleBin",
        "ec2:SearchLocalGatewayRoutes",
        "ec2:SearchTransitGatewayRoutes",
        "ec2messages:Get*",
        "ecr-public:BatchCheckLayerAvailability",
        "ecr-public:DescribeImageTags",
        "ecr-public:DescribeImages",
        "ecr-public:DescribeRegistries",
        "ecr-public:DescribeRepositories",
        "ecr-public:GetAuthorizationToken",
        "ecr-public:GetRegistryCatalogData",
        "ecr-public:GetRepositoryCatalogData",
```

```
        "ecr-public:GetRepositoryPolicy",
        "ecr-public:ListTagsForResource",
        "ecr:BatchCheck*",
        "ecr:BatchGet*",
        "ecr:Describe*",
        "ecr:Get*",
        "ecr:List*",
        "ecs:Describe*",
        "ecs:List*",
        "eks:Describe*",
        "eks:List*",
        "elasticache:Describe*",
        "elasticache:List*",
        "elasticbeanstalk:Check*",
        "elasticbeanstalk:Describe*",
        "elasticbeanstalk:List*",
        "elasticbeanstalk:Request*",
        "elasticbeanstalk:Retrieve*",
        "elasticbeanstalk:Validate*",
        "elasticfilesystem:Describe*",
        "elasticfilesystem:ListTagsForResource",
        "elasticloadbalancing:Describe*",
        "elasticmapreduce:Describe*",
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:List*",
        "elasticmapreduce:View*",
        "elastictranscoder:List*",
        "elastictranscoder:Read*",
        "elemental-appliances-software:Get*",
        "elemental-appliances-software:List*",
        "emr-containers:DescribeJobRun",
        "emr-containers:DescribeManagedEndpoint",
        "emr-containers:DescribeVirtualCluster",
        "emr-containers:ListJobRuns",
        "emr-containers:ListManagedEndpoints",
        "emr-containers:ListTagsForResource",
        "emr-containers:ListVirtualClusters",
        "emr-serverless:GetApplication",
        "emr-serverless:GetDashboardForJobRun",
        "emr-serverless:GetJobRun",
        "emr-serverless:ListApplications",
        "emr-serverless:ListJobRuns",
        "emr-serverless:ListTagsForResource",
        "es:Describe*",
```

```
        "es:ESHttpGet",
        "es:ESHttpHead",
        "es:Get*",
        "es:List*",
        "events:Describe*",
        "events:List*",
        "events:Test*",
        "evidently:GetExperiment",
        "evidently:GetExperimentResults",
        "evidently:GetFeature",
        "evidently:GetLaunch",
        "evidently:GetProject",
        "evidently:GetSegment",
        "evidently:ListExperiments",
        "evidently:ListFeatures",
        "evidently:ListLaunches",
        "evidently:ListProjects",
        "evidently:ListSegmentReferences",
        "evidently:ListSegments",
        "evidently:ListTagsForResource",
        "evidently:TestSegmentPattern",
        "firehose:Describe*",
        "firehose:List*",
        "fis:GetAction",
        "fis:GetExperiment",
        "fis:GetExperimentTargetAccountConfiguration",
        "fis:GetExperimentTemplate",
        "fis:GetTargetAccountConfiguration",
        "fis:GetTargetResourceType",
        "fis:ListActions",
        "fis:ListExperimentResolvedTargets",
        "fis:ListExperimentTargetAccountConfigurations",
        "fis:ListExperimentTemplates",
        "fis:ListExperiments",
        "fis:ListTagsForResource",
        "fis:ListTargetAccountConfigurations",
        "fis:ListTargetResourceTypes",
        "fms:GetAdminAccount",
        "fms:GetAdminScope",
        "fms:GetAppsList",
        "fms:GetComplianceDetail",
        "fms:GetNotificationChannel",
        "fms:GetPolicy",
        "fms:GetProtectionStatus",
```

```
        "fms:GetProtocolsList",
        "fms:GetViolationDetails",
        "fms:ListAppsLists",
        "fms:ListComplianceStatus",
        "fms:ListMemberAccounts",
        "fms:ListPolicies",
        "fms:ListProtocolsLists",
        "fms:ListTagsForResource",
        "forecast:DescribeAutoPredictor",
        "forecast:DescribeDataset",
        "forecast:DescribeDatasetGroup",
        "forecast:DescribeDatasetImportJob",
        "forecast:DescribeExplainability",
        "forecast:DescribeExplainabilityExport",
        "forecast:DescribeForecast",
        "forecast:DescribeForecastExportJob",
        "forecast:DescribeMonitor",
        "forecast:DescribePredictor",
        "forecast:DescribePredictorBacktestExportJob",
        "forecast:DescribeWhatIfAnalysis",
        "forecast:DescribeWhatIfForecast",
        "forecast:DescribeWhatIfForecastExport",
        "forecast:GetAccuracyMetrics",
        "forecast:ListDatasetGroups",
        "forecast:ListDatasetImportJobs",
        "forecast:ListDatasets",
        "forecast:ListExplainabilities",
        "forecast:ListExplainabilityExports",
        "forecast:ListForecastExportJobs",
        "forecast:ListForecasts",
        "forecast:ListMonitorEvaluations",
        "forecast:ListMonitors",
        "forecast:ListPredictorBacktestExportJobs",
        "forecast:ListPredictors",
        "forecast:ListWhatIfAnalyses",
        "forecast:ListWhatIfForecastExports",
        "forecast:ListWhatIfForecasts",
        "forecast:QueryForecast",
        "forecast:QueryWhatIfForecast",
        "frauddetector:BatchGetVariable",
        "frauddetector:DescribeDetector",
        "frauddetector:DescribeModelVersions",
        "frauddetector:GetBatchImportJobs",
        "frauddetector:GetBatchPredictionJobs",
```

```
        "frauddetector:GetDeleteEventsByEventTypeStatus",
        "frauddetector:GetDetectorVersion",
        "frauddetector:GetDetectors",
        "frauddetector:GetEntityTypes",
        "frauddetector:GetEvent",
        "frauddetector:GetEventPredictionMetadata",
        "frauddetector:GetEventTypes",
        "frauddetector:GetExternalModels",
        "frauddetector:GetKMSEncryptionKey",
        "frauddetector:GetLabels",
        "frauddetector:GetListElements",
        "frauddetector:GetListsMetadata",
        "frauddetector:GetModelVersion",
        "frauddetector:GetModels",
        "frauddetector:GetOutcomes",
        "frauddetector:GetRules",
        "frauddetector:GetVariables",
        "frauddetector:ListEventPredictions",
        "frauddetector:ListTagsForResource",
        "freertos:Describe*",
        "freertos:List*",
        "freetier:GetFreeTierAlertPreference",
        "freetier:GetFreeTierUsage",
        "freetier:GetAccountActivity",
        "freetier:GetAccountPlanState",
        "freetier:ListAccountActivities",
        "fsx:Describe*",
        "fsx:List*",
        "gamelift:Describe*",
        "gamelift:Get*",
        "gamelift:List*",
        "gamelift:ResolveAlias",
        "gamelift:Search*",
        "glacier:Describe*",
        "glacier:Get*",
        "glacier:List*",
        "globalaccelerator:Describe*",
        "globalaccelerator:List*",
        "glue:BatchGetCrawlers",
        "glue:BatchGetDevEndpoints",
        "glue:BatchGetJobs",
        "glue:BatchGetPartition",
        "glue:BatchGetTableOptimizer",
        "glue:BatchGetTriggers",
```

```
        "glue:BatchGetWorkflows",
        "glue:CheckSchemaVersionValidity",
        "glue:GetCatalogImportStatus",
        "glue:GetClassifier",
        "glue:GetClassifiers",
        "glue:GetCrawler",
        "glue:GetCrawlerMetrics",
        "glue:GetCrawlers",
        "glue:GetDataCatalogEncryptionSettings",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetDataflowGraph",
        "glue:GetDevEndpoint",
        "glue:GetDevEndpoints",
        "glue:GetJob",
        "glue:GetJobBookmark",
        "glue:GetJobRun",
        "glue:GetJobRuns",
        "glue:GetJobs",
        "glue:GetMLTaskRun",
        "glue:GetMLTaskRuns",
        "glue:GetMLTransform",
        "glue:GetMLTransforms",
        "glue:GetMapping",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetPlan",
        "glue:GetRegistry",
        "glue:GetResourcePolicy",
        "glue:GetSchema",
        "glue:GetSchemaByDefinition",
        "glue:GetSchemaVersion",
        "glue:GetSchemaVersionsDiff",
        "glue:GetSecurityConfiguration",
        "glue:GetSecurityConfigurations",
        "glue:GetSession",
        "glue:GetStatement",
        "glue:GetTable",
        "glue:GetTableOptimizer",
        "glue:GetTableVersion",
        "glue:GetTableVersions",
        "glue:GetTables",
        "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:ListSchemaVersions",
            "glue:ListSchemas",
            "glue:ListSessions",
            "glue:ListStatements",
            "glue:ListTableOptimizerRuns",
            "glue:ListTriggers",
            "glue:ListWorkflows",
            "glue:QuerySchemaVersionMetadata",
            "glue:SearchTables",
            "grafana:DescribeWorkspace",
            "grafana:DescribeWorkspaceAuthentication",
            "grafana:DescribeWorkspaceConfiguration",
            "grafana:ListPermissions",
            "grafana:ListTagsForResource",
            "grafana:ListVersions",
            "grafana:ListWorkspaces",
            "greengrass:DescribeComponent",
            "greengrass:Get*",
            "greengrass:List*",
            "groundstation:DescribeContact",
            "groundstation:GetConfig",
            "groundstation:GetDataflowEndpointGroup",
            "groundstation:GetMinuteUsage",
            "groundstation:GetMissionProfile",
            "groundstation:GetSatellite",
            "groundstation:ListConfigs",
            "groundstation:ListContacts",
            "groundstation:ListDataflowEndpointGroups",
            "groundstation:ListGroundStations",
            "groundstation:ListMissionProfiles",
            "groundstation:ListSatellites",
```

```
        "groundstation:ListTagsForResource",
        "guardduty:Describe*",
        "guardduty:Get*",
        "guardduty:List*",
        "health:Describe*",
        "healthlake:DescribeFHIRDatastore",
        "healthlake:DescribeFHIRExportJob",
        "healthlake:DescribeFHIRImportJob",
        "healthlake:GetCapabilities",
        "healthlake:ListFHIRDatastores",
        "healthlake:ListFHIRExportJobs",
        "healthlake:ListFHIRImportJobs",
        "healthlake:ListTagsForResource",
        "healthlake:ReadResource",
        "healthlake:SearchWithGet",
        "healthlake:SearchWithPost",
        "iam:Generate*",
        "iam:Get*",
        "iam:List*",
        "iam:Simulate*",
        "identity-sync:GetSyncProfile",
        "identity-sync:GetSyncTarget",
        "identity-sync:ListSyncFilters",
        "identitystore-auth:BatchGetSession",
        "identitystore-auth:ListSessions",
        "identitystore:DescribeGroup",
        "identitystore:DescribeGroupMembership",
        "identitystore:DescribeUser",
        "identitystore:GetGroupId",
        "identitystore:GetGroupMembershipId",
        "identitystore:GetUserId",
        "identitystore:IsMemberInGroups",
        "identitystore:ListGroupMemberships",
        "identitystore:ListGroupMembershipsForMember",
        "identitystore:ListGroups",
        "identitystore:ListUsers",
        "imagebuilder:Get*",
        "imagebuilder:List*",
        "importexport:Get*",
        "importexport:List*",
        "inspector2:BatchGetAccountStatus",
        "inspector2:BatchGetCodeSnippet",
        "inspector2:BatchGetFreeTrialInfo",
        "inspector2:BatchGetMemberEc2DeepInspectionStatus",
```

```
        "inspector2:DescribeOrganizationConfiguration",
        "inspector2:GetCisScanReport",
        "inspector2:GetConfiguration",
        "inspector2:GetDelegatedAdminAccount",
        "inspector2:GetEc2DeepInspectionConfiguration",
        "inspector2:GetEncryptionKey",
        "inspector2:GetFindingsReportStatus",
        "inspector2:GetMember",
        "inspector2:GetSbomExport",
        "inspector2:ListAccountPermissions",
        "inspector2:ListCisScanConfigurations",
        "inspector2:ListCisScans",
        "inspector2:ListCoverage",
        "inspector2:ListCoverageStatistics",
        "inspector2:ListDelegatedAdminAccounts",
        "inspector2:ListFilters",
        "inspector2:ListFindingAggregations",
        "inspector2:ListFindings",
        "inspector2:ListMembers",
        "inspector2:ListTagsForResource",
        "inspector2:ListUsageTotals",
        "inspector2:SearchVulnerabilities",
        "inspector:Describe*",
        "inspector:Get*",
        "inspector:List*",
        "inspector:Preview*",
        "internetmonitor:GetHealthEvent",
        "internetmonitor:GetInternetEvent",
        "internetmonitor:GetMonitor",
        "internetmonitor:ListHealthEvents",
        "internetmonitor:ListInternetEvents",
        "internetmonitor:ListMonitors",
        "internetmonitor:ListTagsForResource",
        "invoicing:GetInvoiceEmailDeliveryPreferences",
        "invoicing:GetInvoicePDF",
        "invoicing:ListInvoiceSummaries",
        "iot1click:DescribeDevice",
        "iot1click:DescribePlacement",
        "iot1click:DescribeProject",
        "iot1click:GetDeviceMethods",
        "iot1click:GetDevicesInPlacement",
        "iot1click:ListDeviceEvents",
        "iot1click:ListDevices",
        "iot1click:ListPlacements",
```

```
        "iot1click:ListProjects",
        "iot1click:ListTagsForResource",
        "iot:Describe*",
        "iot:Get*",
        "iot:List*",
        "iotanalytics:Describe*",
        "iotanalytics:Get*",
        "iotanalytics:List*",
        "iotanalytics:SampleChannelData",
        "iotevents:DescribeAlarm",
        "iotevents:DescribeAlarmModel",
        "iotevents:DescribeDetector",
        "iotevents:DescribeDetectorModel",
        "iotevents:DescribeInput",
        "iotevents:DescribeLoggingOptions",
        "iotevents:ListAlarmModelVersions",
        "iotevents:ListAlarmModels",
        "iotevents:ListAlarms",
        "iotevents:ListDetectorModelVersions",
        "iotevents:ListDetectorModels",
        "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:ListDecoderManifestSignals",
        "iotfleetwise:ListDecoderManifests",
        "iotfleetwise:ListFleets",
        "iotfleetwise:ListFleetsForVehicle",
        "iotfleetwise:ListModelManifestNodes",
        "iotfleetwise:ListModelManifests",
        "iotfleetwise:ListSignalCatalogNodes",
        "iotfleetwise:ListSignalCatalogs",
```

```
        "iotfleetwise:ListTagsForResource",
        "iotfleetwise:ListVehicles",
        "iotfleetwise:ListVehiclesInFleet",
        "iotsitewise:Describe*",
        "iotsitewise:Get*",
        "iotsitewise:List*",
        "iotwireless:GetDestination",
        "iotwireless:GetDeviceProfile",
        "iotwireless:GetEventConfigurationByResourceTypes",
        "iotwireless:GetFuotaTask",
        "iotwireless:GetLogLevelsByResourceTypes",
        "iotwireless:GetMetricConfiguration",
        "iotwireless:GetMetrics",
        "iotwireless:GetMulticastGroup",
        "iotwireless:GetMulticastGroupSession",
        "iotwireless:GetNetworkAnalyzerConfiguration",
        "iotwireless:GetPartnerAccount",
        "iotwireless:GetPosition",
        "iotwireless:GetPositionConfiguration",
        "iotwireless:GetPositionEstimate",
        "iotwireless:GetResourceEventConfiguration",
        "iotwireless:GetResourceLogLevel",
        "iotwireless:GetResourcePosition",
        "iotwireless:GetServiceEndpoint",
        "iotwireless:GetServiceProfile",
        "iotwireless:GetWirelessDevice",
        "iotwireless:GetWirelessDeviceImportTask",
        "iotwireless:GetWirelessDeviceStatistics",
        "iotwireless:GetWirelessGateway",
        "iotwireless:GetWirelessGatewayCertificate",
        "iotwireless:GetWirelessGatewayFirmwareInformation",
        "iotwireless:GetWirelessGatewayStatistics",
        "iotwireless:GetWirelessGatewayTask",
        "iotwireless:GetWirelessGatewayTaskDefinition",
        "iotwireless:ListDestinations",
        "iotwireless:ListDeviceProfiles",
        "iotwireless:ListDevicesForWirelessDeviceImportTask",
        "iotwireless:ListEventConfigurations",
        "iotwireless:ListFuotaTasks",
        "iotwireless:ListMulticastGroups",
        "iotwireless:ListMulticastGroupsByFuotaTask",
        "iotwireless:ListNetworkAnalyzerConfigurations",
        "iotwireless:ListPartnerAccounts",
        "iotwireless:ListPositionConfigurations",
```

```
        "iotwireless:ListQueuedMessages",
        "iotwireless:ListServiceProfiles",
        "iotwireless:ListTagsForResource",
        "iotwireless:ListWirelessDeviceImportTasks",
        "iotwireless:ListWirelessDevices",
        "iotwireless:ListWirelessGatewayTaskDefinitions",
        "iotwireless:ListWirelessGateways",
        "ivs:BatchGetChannel",
        "ivs:GetChannel",
        "ivs:GetComposition",
        "ivs:GetEncoderConfiguration",
        "ivs:GetIngestConfiguration",
        "ivs:GetParticipant",
        "ivs:GetPlaybackKeyPair",
        "ivs:GetPlaybackRestrictionPolicy",
        "ivs:GetPublicKey",
        "ivs:GetRecordingConfiguration",
        "ivs:GetStage",
        "ivs:GetStageSession",
        "ivs:GetStorageConfiguration",
        "ivs:GetStream",
        "ivs:GetStreamSession",
        "ivs:ListChannels",
        "ivs:ListCompositions",
        "ivs:ListEncoderConfigurations",
        "ivs:ListIngestConfigurations",
        "ivs:ListParticipantEvents",
        "ivs:ListParticipants",
        "ivs:ListPlaybackKeyPairs",
        "ivs:ListPlaybackRestrictionPolicies",
        "ivs:ListPublicKeys",
        "ivs:ListRecordingConfigurations",
        "ivs:ListStageSessions",
        "ivs:ListStages",
        "ivs:ListStorageConfigurations",
        "ivs:ListStreamKeys",
        "ivs:ListStreamSessions",
        "ivs:ListStreams",
        "ivs:ListTagsForResource",
        "ivschat:GetLoggingConfiguration",
        "ivschat:GetRoom",
        "ivschat:ListLoggingConfigurations",
        "ivschat:ListRooms",
        "ivschat:ListTagsForResource"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ReadOnlyActionsGroup2",
      "Effect" : "Allow",
      "Action" : [
        "kafka:Describe*",
        "kafka:DescribeCluster",
        "kafka:DescribeClusterOperation",
        "kafka:DescribeClusterV2",
        "kafka:DescribeConfiguration",
        "kafka:DescribeConfigurationRevision",
        "kafka:Get*",
        "kafka:GetBootstrapBrokers",
        "kafka:GetCompatibleKafkaVersions",
        "kafka:List*",
        "kafka:ListClusterOperations",
        "kafka:ListClusters",
        "kafka:ListClustersV2",
        "kafka:ListConfigurationRevisions",
        "kafka:ListConfigurations",
        "kafka:ListKafkaVersions",
        "kafka:ListNodes",
        "kafka:ListTagsForResource",
        "kafkaconnect:DescribeConnector",
        "kafkaconnect:DescribeCustomPlugin",
        "kafkaconnect:DescribeWorkerConfiguration",
        "kafkaconnect:ListConnectors",
        "kafkaconnect:ListCustomPlugins",
        "kafkaconnect:ListWorkerConfigurations",
        "kendra:BatchGetDocumentStatus",
        "kendra:DescribeDataSource",
        "kendra:DescribeExperience",
        "kendra:DescribeFaq",
        "kendra:DescribeIndex",
        "kendra:DescribePrincipalMapping",
        "kendra:DescribeQuerySuggestionsBlockList",
        "kendra:DescribeQuerySuggestionsConfig",
        "kendra:DescribeThesaurus",
        "kendra:GetQuerySuggestions",
        "kendra:GetSnapshots",
        "kendra:ListDataSourceSyncJobs",
        "kendra:ListDataSources",
```

```
        "kendra:ListEntityPersonas",
        "kendra:ListExperienceEntities",
        "kendra:ListExperiences",
        "kendra:ListFaqs",
        "kendra:ListGroupsOlderThanOrderingId",
        "kendra:ListIndices",
        "kendra:ListQuerySuggestionsBlockLists",
        "kendra:ListTagsForResource",
        "kendra:ListThesauri",
        "kendra:Query",
        "kinesis:Describe*",
        "kinesis:Get*",
        "kinesis:List*",
        "kinesisanalytics:Describe*",
        "kinesisanalytics:Discover*",
        "kinesisanalytics:Get*",
        "kinesisanalytics:List*",
        "kinesisvideo:Describe*",
        "kinesisvideo:Get*",
        "kinesisvideo:List*",
        "kms:Describe*",
        "kms:Get*",
        "kms:List*",
        "lakeformation:DescribeResource",
        "lakeformation:GetDataCellsFilter",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:GetEffectivePermissionsForPath",
        "lakeformation:GetLfTag",
        "lakeformation:GetResourceLfTags",
        "lakeformation:ListDataCellsFilter",
        "lakeformation:ListLfTags",
        "lakeformation:ListPermissions",
        "lakeformation:ListResources",
        "lakeformation:ListTableStorageOptimizers",
        "lakeformation:SearchDatabasesByLfTags",
        "lakeformation:SearchTablesByLfTags",
        "lambda:Get*",
        "lambda:List*",
        "launchwizard:DescribeAdditionalNode",
        "launchwizard:DescribeProvisionedApp",
        "launchwizard:DescribeProvisioningEvents",
        "launchwizard:DescribeSettingsSet",
        "launchwizard:GetDeployment",
        "launchwizard:GetInfrastructureSuggestion",
```

```
        "launchwizard:GetIpAddress",
        "launchwizard:GetResourceCostEstimate",
        "launchwizard:GetResourceRecommendation",
        "launchwizard:GetSettingsSet",
        "launchwizard:GetWorkload",
        "launchwizard:GetWorkloadAsset",
        "launchwizard:GetWorkloadAssets",
        "launchwizard:GetWorkloadDeploymentPattern",
        "launchwizard:ListAdditionalNodes",
        "launchwizard:ListAllowedResources",
        "launchwizard:ListDeploymentEvents",
        "launchwizard:ListDeployments",
        "launchwizard:ListProvisionedApps",
        "launchwizard:ListResourceCostEstimates",
        "launchwizard:ListSettingsSets",
        "launchwizard:ListTagsForResource",
        "launchwizard:ListWorkloadDeploymentOptions",
        "launchwizard:ListWorkloadDeploymentPatterns",
        "launchwizard:ListWorkloads",
        "lex:DescribeBot",
        "lex:DescribeBotAlias",
        "lex:DescribeBotChannel",
        "lex:DescribeBotLocale",
        "lex:DescribeBotReplica",
        "lex:DescribeBotVersion",
        "lex:DescribeExport",
        "lex:DescribeImport",
        "lex:DescribeIntent",
        "lex:DescribeResourcePolicy",
        "lex:DescribeSlot",
        "lex:DescribeSlotType",
        "lex:Get*",
        "lex:ListBotAliasReplicas",
        "lex:ListBotAliases",
        "lex:ListBotChannels",
        "lex:ListBotLocales",
        "lex:ListBotReplicas",
        "lex:ListBotVersionReplicas",
        "lex:ListBotVersions",
        "lex:ListBots",
        "lex:ListBuiltInIntents",
        "lex:ListBuiltInSlotTypes",
        "lex:ListExports",
        "lex:ListImports",
```

```
        "lex:ListIntents",
        "lex:ListSlotTypes",
        "lex:ListSlots",
        "lex:ListTagsForResource",
        "license-manager:Get*",
        "license-manager:List*",
        "lightsail:GetActiveNames",
        "lightsail:GetAlarms",
        "lightsail:GetAutoSnapshots",
        "lightsail:GetBlueprints",
        "lightsail:GetBucketAccessKeys",
        "lightsail:GetBucketBundles",
        "lightsail:GetBucketMetricData",
        "lightsail:GetBuckets",
        "lightsail:GetBundles",
        "lightsail:GetCertificates",
        "lightsail:GetCloudFormationStackRecords",
        "lightsail:GetContainerAPIMetadata",
        "lightsail:GetContainerImages",
        "lightsail:GetContainerServiceDeployments",
        "lightsail:GetContainerServiceMetricData",
        "lightsail:GetContainerServicePowers",
        "lightsail:GetContainerServices",
        "lightsail:GetDisk",
        "lightsail:GetDiskSnapshot",
        "lightsail:GetDiskSnapshots",
        "lightsail:GetDisks",
        "lightsail:GetDistributionBundles",
        "lightsail:GetDistributionLatestCacheReset",
        "lightsail:GetDistributionMetricData",
        "lightsail:GetDistributions",
        "lightsail:GetDomain",
        "lightsail:GetDomains",
        "lightsail:GetExportSnapshotRecords",
        "lightsail:GetInstance",
        "lightsail:GetInstanceMetricData",
        "lightsail:GetInstancePortStates",
        "lightsail:GetInstanceSnapshot",
        "lightsail:GetInstanceSnapshots",
        "lightsail:GetInstanceState",
        "lightsail:GetInstances",
        "lightsail:GetKeyPair",
        "lightsail:GetKeyPairs",
        "lightsail:GetLoadBalancer",
```

```
        "lightsail:GetLoadBalancerMetricData",
        "lightsail:GetLoadBalancerTlsCertificates",
        "lightsail:GetLoadBalancers",
        "lightsail:GetOperation",
        "lightsail:GetOperations",
        "lightsail:GetOperationsForResource",
        "lightsail:GetRegions",
        "lightsail:GetRelationalDatabase",
        "lightsail:GetRelationalDatabaseBlueprints",
        "lightsail:GetRelationalDatabaseBundles",
        "lightsail:GetRelationalDatabaseEvents",
        "lightsail:GetRelationalDatabaseLogEvents",
        "lightsail:GetRelationalDatabaseLogStreams",
        "lightsail:GetRelationalDatabaseMetricData",
        "lightsail:GetRelationalDatabaseParameters",
        "lightsail:GetRelationalDatabaseSnapshot",
        "lightsail:GetRelationalDatabaseSnapshots",
        "lightsail:GetRelationalDatabases",
        "lightsail:GetStaticIp",
        "lightsail:GetStaticIps",
        "lightsail:Is*",
        "logs:Describe*",
        "logs:FilterLogEvents",
        "logs:Get*",
        "logs:ListAnomalies",
        "logs:ListEntitiesForLogGroup",
        "logs:ListIntegrations",
        "logs:ListLogAnomalyDetectors",
        "logs:ListLogDeliveries",
        "logs:ListLogGroupsForEntity",
        "logs:ListLogGroupsForQuery",
        "logs:ListTagsForResource",
        "logs:ListTagsLogGroup",
        "logs:StartLiveTail",
        "logs:StartQuery",
        "logs:StopLiveTail",
        "logs:StopQuery",
        "logs:TestMetricFilter",
        "logs:ListAggregateLogGroupSummaries",
        "logs:ListSourcesForS3TableIntegration",
        "logs:ListScheduledQueries",
        "lookoutequipment:DescribeDataIngestionJob",
        "lookoutequipment:DescribeDataset",
        "lookoutequipment:DescribeInferenceScheduler",
```

```
        "lookoutequipment:DescribeLabel",
        "lookoutequipment:DescribeLabelGroup",
        "lookoutequipment:DescribeModel",
        "lookoutequipment:DescribeModelVersion",
        "lookoutequipment:DescribeResourcePolicy",
        "lookoutequipment:DescribeRetrainingScheduler",
        "lookoutequipment:ListDataIngestionJobs",
        "lookoutequipment:ListDatasets",
        "lookoutequipment:ListInferenceEvents",
        "lookoutequipment:ListInferenceExecutions",
        "lookoutequipment:ListInferenceSchedulers",
        "lookoutequipment:ListLabelGroups",
        "lookoutequipment:ListLabels",
        "lookoutequipment:ListModelVersions",
        "lookoutequipment:ListModels",
        "lookoutequipment:ListRetrainingSchedulers",
        "lookoutequipment:ListSensorStatistics",
        "lookoutequipment:ListTagsForResource",
        "lookoutmetrics:Describe*",
        "lookoutmetrics:Get*",
        "lookoutmetrics:List*",
        "lookoutvision:DescribeDataset",
        "lookoutvision:DescribeModel",
        "lookoutvision:DescribeModelPackagingJob",
        "lookoutvision:DescribeProject",
        "lookoutvision:ListDatasetEntries",
        "lookoutvision:ListModelPackagingJobs",
        "lookoutvision:ListModels",
        "lookoutvision:ListProjects",
        "lookoutvision:ListTagsForResource",
        "m2:GetApplication",
        "m2:GetApplicationVersion",
        "m2:GetBatchJobExecution",
        "m2:GetDataSetDetails",
        "m2:GetDataSetImportTask",
        "m2:GetDeployment",
        "m2:GetEnvironment",
        "m2:ListApplicationVersions",
        "m2:ListApplications",
        "m2:ListBatchJobDefinitions",
        "m2:ListBatchJobExecutions",
        "m2:ListDataSetImportHistory",
        "m2:ListDataSets",
        "m2:ListDeployments",
```

```
        "m2:ListEngineVersions",
        "m2:ListEnvironments",
        "m2:ListTagsForResource",
        "machinelearning:Describe*",
        "machinelearning:Get*",
        "macie2:BatchGetCustomDataIdentifiers",
        "macie2:DescribeBuckets",
        "macie2:DescribeClassificationJob",
        "macie2:DescribeOrganizationConfiguration",
        "macie2:GetAdministratorAccount",
        "macie2:GetAllowList",
        "macie2:GetAutomatedDiscoveryConfiguration",
        "macie2:GetBucketStatistics",
        "macie2:GetClassificationExportConfiguration",
        "macie2:GetClassificationScope",
        "macie2:GetCustomDataIdentifier",
        "macie2:GetFindingStatistics",
        "macie2:GetFindings",
        "macie2:GetFindingsFilter",
        "macie2:GetFindingsPublicationConfiguration",
        "macie2:GetInvitationsCount",
        "macie2:GetMacieSession",
        "macie2:GetMember",
        "macie2:GetResourceProfile",
        "macie2:GetRevealConfiguration",
        "macie2:GetSensitiveDataOccurrencesAvailability",
        "macie2:GetSensitivityInspectionTemplate",
        "macie2:GetUsageStatistics",
        "macie2:GetUsageTotals",
        "macie2:ListAllowLists",
        "macie2:ListAutomatedDiscoveryAccounts",
        "macie2:ListClassificationJobs",
        "macie2:ListClassificationScopes",
        "macie2:ListCustomDataIdentifiers",
        "macie2:ListFindings",
        "macie2:ListFindingsFilters",
        "macie2:ListInvitations",
        "macie2:ListMembers",
        "macie2:ListOrganizationAdminAccounts",
        "macie2:ListResourceProfileArtifacts",
        "macie2:ListResourceProfileDetections",
        "macie2:ListSensitivityInspectionTemplates",
        "macie2:ListTagsForResource",
        "macie2:SearchResources",
```

```
        "managedblockchain:GetMember",
        "managedblockchain:GetNetwork",
        "managedblockchain:GetNode",
        "managedblockchain:GetProposal",
        "managedblockchain:ListInvitations",
        "managedblockchain:ListMembers",
        "managedblockchain:ListNetworks",
        "managedblockchain:ListNodes",
        "managedblockchain:ListProposalVotes",
        "managedblockchain:ListProposals",
        "managedblockchain:ListTagsForResource",
        "mediaconnect:DescribeFlow",
        "mediaconnect:DescribeOffering",
        "mediaconnect:DescribeReservation",
        "mediaconnect:ListEntitlements",
        "mediaconnect:ListFlows",
        "mediaconnect:ListOfferings",
        "mediaconnect:ListReservations",
        "mediaconnect:ListTagsForResource",
        "mediaconvert:DescribeEndpoints",
        "mediaconvert:Get*",
        "mediaconvert:List*",
        "medialive:DescribeAccountConfiguration",
        "medialive:DescribeChannel",
        "medialive:DescribeChannelPlacementGroup",
        "medialive:DescribeCluster",
        "medialive:DescribeInput",
        "medialive:DescribeInputDevice",
        "medialive:DescribeInputDeviceThumbnail",
        "medialive:DescribeInputSecurityGroup",
        "medialive:DescribeMultiplex",
        "medialive:DescribeMultiplexProgram",
        "medialive:DescribeNetwork",
        "medialive:DescribeOffering",
        "medialive:DescribeReservation",
        "medialive:DescribeSchedule",
        "medialive:GetCloudWatchAlarmTemplate",
        "medialive:GetCloudWatchAlarmTemplateGroup",
        "medialive:GetEventBridgeRuleTemplate",
        "medialive:GetEventBridgeRuleTemplateGroup",
        "medialive:GetSignalMap",
        "medialive:ListChannels",
        "medialive:ListCloudWatchAlarmTemplateGroups",
        "medialive:ListCloudWatchAlarmTemplates",
```

```
        "medialive:ListEventBridgeRuleTemplateGroups",
        "medialive:ListEventBridgeRuleTemplates",
        "medialive:ListInputDevices",
        "medialive:ListInputDeviceTransfers",
        "medialive:ListInputs",
        "medialive:ListInputSecurityGroups",
        "medialive:ListMultiplexes",
        "medialive:ListMultiplexPrograms",
        "medialive:ListOfferings",
        "medialive:ListReservations",
        "medialive:ListSignalMaps",
        "medialive:ListTagsForResource",
        "mediapackage-vod:Describe*",
        "mediapackage-vod:List*",
        "mediapackage:Describe*",
        "mediapackage:List*",
        "mediapackagev2:GetChannel",
        "mediapackagev2:GetChannelGroup",
        "mediapackagev2:GetChannelPolicy",
        "mediapackagev2:GetHeadObject",
        "mediapackagev2:GetObject",
        "mediapackagev2:GetOriginEndpoint",
        "mediapackagev2:GetOriginEndpointPolicy",
        "mediapackagev2:ListChannelGroups",
        "mediapackagev2:ListChannels",
        "mediapackagev2:ListOriginEndpoints",
        "mediapackagev2:ListTagsForResource",
        "mediastore:DescribeContainer",
        "mediastore:DescribeObject",
        "mediastore:GetContainerPolicy",
        "mediastore:GetCorsPolicy",
        "mediastore:GetLifecyclePolicy",
        "mediastore:GetMetricPolicy",
        "mediastore:GetObject",
        "mediastore:ListContainers",
        "mediastore:ListItems",
        "mediastore:ListTagsForResource",
        "memorydb:DescribeAcls",
        "memorydb:DescribeClusters",
        "memorydb:DescribeEngineVersions",
        "memorydb:DescribeEvents",
        "memorydb:DescribeMultiRegionClusters",
        "memorydb:DescribeMultiRegionParameterGroups",
        "memorydb:DescribeMultiRegionParameters",
```

```
        "memorydb:DescribeParameterGroups",
        "memorydb:DescribeParameters",
        "memorydb:DescribeReservedNodes",
        "memorydb:DescribeReservedNodesOfferings",
        "memorydb:DescribeServiceUpdates",
        "memorydb:DescribeSnapshots",
        "memorydb:DescribeSubnetGroups",
        "memorydb:DescribeUsers",
        "memorydb:ListAllowedMultiRegionClusterUpdates",
        "memorydb:ListAllowedNodeTypeUpdates",
        "memorydb:ListTags",
        "mgh:Describe*",
        "mgh:GetHomeRegion",
        "mgh:List*",
        "mgn:DescribeJobLogItems",
        "mgn:DescribeJobs",
        "mgn:DescribeLaunchConfigurationTemplates",
        "mgn:DescribeReplicationConfigurationTemplates",
        "mgn:DescribeSourceServers",
        "mgn:DescribeVcenterClients",
        "mgn:GetLaunchConfiguration",
        "mgn:GetReplicationConfiguration",
        "mgn:ListApplications",
        "mgn:ListSourceServerActions",
        "mgn:ListTemplateActions",
        "mgn:ListWaves",
        "mobileanalytics:Get*",
        "mobiletargeting:Get*",
        "mobiletargeting:List*",
        "monitron:GetProject",
        "monitron:GetProjectAdminUser",
        "monitron:ListProjects",
        "monitron:ListTagsForResource",
        "mpa:GetApprovalTeam",
        "mpa:GetIdentitySource",
        "mpa:GetPolicyVersion",
        "mpa:GetResourcePolicy",
        "mpa:GetSession",
        "mpa:ListApprovalTeams",
        "mpa:ListIdentitySources",
        "mpa:ListPolicies",
        "mpa:ListPolicyVersions",
        "mpa:ListResourcePolicies",
        "mpa:ListSessions",
```

```
        "mpa:ListTagsForResource",
        "mq:Describe*",
        "mq:List*",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeLoggingConfiguration",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:DescribeRuleGroupMetadata",
        "network-firewall:DescribeTLSInspectionConfiguration",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups",
        "network-firewall:ListTLSInspectionConfigurations",
        "network-firewall:ListTagsForResource",
        "networkflowmonitor:GetMonitor",
        "networkflowmonitor:GetScope",
        "networkflowmonitor:ListMonitors",
        "networkflowmonitor:ListScopes",
        "networkmanager:DescribeGlobalNetworks",
        "networkmanager:GetConnectAttachment",
        "networkmanager:GetConnectPeer",
        "networkmanager:GetConnectPeerAssociations",
        "networkmanager:GetConnections",
        "networkmanager:GetCoreNetwork",
        "networkmanager:GetCoreNetworkChangeEvents",
        "networkmanager:GetCoreNetworkChangeSet",
        "networkmanager:GetCoreNetworkPolicy",
        "networkmanager:GetCustomerGatewayAssociations",
        "networkmanager:GetDevices",
        "networkmanager:GetLinkAssociations",
        "networkmanager:GetLinks",
        "networkmanager:GetNetworkResourceCounts",
        "networkmanager:GetNetworkResourceRelationships",
        "networkmanager:GetNetworkResources",
        "networkmanager:GetNetworkRoutes",
        "networkmanager:GetNetworkTelemetry",
        "networkmanager:GetResourcePolicy",
        "networkmanager:GetRouteAnalysis",
        "networkmanager:GetSiteToSiteVpnAttachment",
        "networkmanager:GetSites",
        "networkmanager:GetTransitGatewayConnectPeerAssociations",
        "networkmanager:GetTransitGatewayPeering",
        "networkmanager:GetTransitGatewayRegistrations",
```

```
        "networkmanager:GetTransitGatewayRouteTableAttachment",
        "networkmanager:GetVpcAttachment",
        "networkmanager:ListAttachments",
        "networkmanager:ListConnectPeers",
        "networkmanager:ListCoreNetworkPolicyVersions",
        "networkmanager:ListCoreNetworks",
        "networkmanager:ListPeerings",
        "networkmanager:ListTagsForResource",
        "networkmonitor:GetMonitor",
        "networkmonitor:GetProbe",
        "networkmonitor:ListMonitors",
        "networkmonitor:ListTagsForResource",
        "nimble:GetEula",
        "nimble:GetFeatureMap",
        "nimble:GetLaunchProfile",
        "nimble:GetLaunchProfileDetails",
        "nimble:GetLaunchProfileInitialization",
        "nimble:GetLaunchProfileMember",
        "nimble:GetStreamingImage",
        "nimble:GetStreamingSession",
        "nimble:GetStudio",
        "nimble:GetStudioComponent",
        "nimble:GetStudioMember",
        "nimble:ListEulaAcceptances",
        "nimble:ListEulas",
        "nimble:ListLaunchProfileMembers",
        "nimble:ListLaunchProfiles",
        "nimble:ListStreamingImages",
        "nimble:ListStreamingSessions",
        "nimble:ListStudioComponents",
        "nimble:ListStudioMembers",
        "nimble:ListStudios",
        "nimble:ListTagsForResource",
        "notifications-contacts:GetEmailContact",
        "notifications-contacts:ListEmailContacts",
        "notifications-contacts:ListTagsForResource",
        "notifications:GetEventRule",
        "notifications:GetFeatureOptInStatus",
        "notifications:GetManagedNotificationChildEvent",
        "notifications:GetManagedNotificationConfiguration",
        "notifications:GetManagedNotificationEvent",
        "notifications:GetNotificationConfiguration",
        "notifications:GetNotificationEvent",
        "notifications:GetNotificationsAccessForOrganization",
```

```
        "notifications:List*",
        "oam:GetLink",
        "oam:GetSink",
        "oam:GetSinkPolicy",
        "oam:ListAttachedLinks",
        "oam:ListLinks",
        "oam:ListSinks",
        "observabilityadmin:GetCentralizationRuleForOrganization",
        "observabilityadmin:GetTelemetryEnrichmentStatus",
        "observabilityadmin:GetTelemetryEvaluationStatus",
        "observabilityadmin:GetTelemetryEvaluationStatusForOrganization",
        "observabilityadmin:GetTelemetryRule",
        "observabilityadmin:GetTelemetryRuleForOrganization",
        "observabilityadmin:ListCentralizationRulesForOrganization",
        "observabilityadmin:ListResourceTelemetry",
        "observabilityadmin:ListResourceTelemetryForOrganization",
        "observabilityadmin:ListTagsForResource",
        "observabilityadmin:ListTelemetryRules",
        "observabilityadmin:ListTelemetryRulesForOrganization",
        "observabilityadmin:GetTelemetryPipeline",
        "observabilityadmin:ListTelemetryPipelines",
        "observabilityadmin:TestTelemetryPipeline",
        "observabilityadmin:ValidateTelemetryPipelineConfiguration",
        "observabilityadmin:ListS3TableIntegrations",
        "observabilityadmin:GetS3TableIntegration",
        "omics:Get*",
        "omics:List*",
        "one:GetDeviceConfigurationTemplate",
        "one:GetDeviceInstance",
        "one:GetDeviceInstanceConfiguration",
        "one:GetSite",
        "one:GetSiteAddress",
        "one:ListDeviceConfigurationTemplates",
        "one:ListDeviceInstances",
        "one:ListSites",
        "one:ListUsers",
        "opsworks-cm:Describe*",
        "opsworks-cm:List*",
        "opsworks:Describe*",
        "opsworks:Get*",
        "organizations:Describe*",
        "organizations:List*",
        "osis:GetPipeline",
        "osis:GetPipelineBlueprint",
```

```
        "osis:GetPipelineChangeProgress",
        "osis:ListPipelineBlueprints",
        "osis:ListPipelines",
        "osis:ListTagsForResource",
        "outposts:Get*",
        "outposts:List*",
        "payment-cryptography:GetAlias",
        "payment-cryptography:GetKey",
        "payment-cryptography:GetPublicKeyCertificate",
        "payment-cryptography:ListAliases",
        "payment-cryptography:ListKeys",
        "payment-cryptography:ListTagsForResource",
        "payments:GetPaymentInstrument",
        "payments:GetPaymentStatus",
        "payments:ListPaymentInstruments",
        "payments:ListPaymentPreferences",
        "payments:ListPaymentProgramOptions",
        "payments:ListPaymentProgramStatus",
        "payments:ListTagsForResource",
        "pca-connector-ad:GetConnector",
        "pca-connector-ad:GetDirectoryRegistration",
        "pca-connector-ad:GetServicePrincipalName",
        "pca-connector-ad:GetTemplate",
        "pca-connector-ad:GetTemplateGroupAccessControlEntry",
        "pca-connector-ad:ListConnectors",
        "pca-connector-ad:ListDirectoryRegistrations",
        "pca-connector-ad:ListServicePrincipalNames",
        "pca-connector-ad:ListTagsForResource",
        "pca-connector-ad:ListTemplateGroupAccessControlEntries",
        "pca-connector-ad:ListTemplates",
        "pca-connector-scep:GetChallengeMetadata",
        "pca-connector-scep:GetConnector",
        "pca-connector-scep:ListChallengeMetadata",
        "pca-connector-scep:ListConnectors",
        "pca-connector-scep:ListTagsForResource",
        "pcs:GetCluster",
        "pcs:GetComputeNodeGroup",
        "pcs:GetQueue",
        "pcs:ListClusters",
        "pcs:ListComputeNodeGroups",
        "pcs:ListQueues",
        "pcs:ListTagsForResource",
        "personalize:Describe*",
        "personalize:Get*",
```

```
        "personalize:List*",
        "pi:DescribeDimensionKeys",
        "pi:GetDimensionKeyDetails",
        "pi:GetResourceMetadata",
        "pi:GetResourceMetrics",
        "pi:ListAvailableResourceDimensions",
        "pi:ListAvailableResourceMetrics",
        "pipes:DescribePipe",
        "pipes:ListPipes",
        "pipes:ListTagsForResource",
        "polly:Describe*",
        "polly:Get*",
        "polly:List*",
        "polly:SynthesizeSpeech",
        "pricing:DescribeServices",
        "pricing:GetAttributeValues",
        "pricing:GetPriceListFileUrl",
        "pricing:GetProducts",
        "pricing:ListPriceLists",
        "proton:GetDeployment",
        "proton:GetEnvironment",
        "proton:GetEnvironmentTemplate",
        "proton:GetEnvironmentTemplateVersion",
        "proton:GetService",
        "proton:GetServiceInstance",
        "proton:GetServiceTemplate",
        "proton:GetServiceTemplateVersion",
        "proton:ListDeployments",
        "proton:ListEnvironmentAccountConnections",
        "proton:ListEnvironmentTemplates",
        "proton:ListEnvironments",
        "proton:ListServiceInstances",
        "proton:ListServiceTemplates",
        "proton:ListServices",
        "proton:ListTagsForResource",
        "purchase-orders:GetPurchaseOrder",
        "purchase-orders:ListPurchaseOrderInvoices",
        "purchase-orders:ListPurchaseOrders",
        "purchase-orders:ViewPurchaseOrders",
        "qbusiness:GetApplication",
        "qbusiness:GetChatControlsConfiguration",
        "qbusiness:GetDataSource",
        "qbusiness:GetGroup",
        "qbusiness:GetIndex",
```

```
        "qbusiness:GetPlugin",
        "qbusiness:GetRetriever",
        "qbusiness:GetUser",
        "qbusiness:GetWebExperience",
        "qbusiness:ListApplications",
        "qbusiness:ListDataSourceSyncJobs",
        "qbusiness:ListDataSources",
        "qbusiness:ListGroups",
        "qbusiness:ListIndices",
        "qbusiness:ListPlugins",
        "qbusiness:ListRetrievers",
        "qbusiness:ListSubscriptions",
        "qbusiness:ListTagsForResource",
        "qbusiness:ListWebExperiences",
        "qldb:DescribeJournalKinesisStream",
        "qldb:DescribeJournalS3Export",
        "qldb:DescribeLedger",
        "qldb:GetBlock",
        "qldb:GetDigest",
        "qldb:GetRevision",
        "qldb:ListJournalKinesisStreamsForLedger",
        "qldb:ListJournalS3Exports",
        "qldb:ListJournalS3ExportsForLedger",
        "qldb:ListLedgers",
        "qldb:ListTagsForResource",
        "ram:Get*",
        "ram:List*",
        "rbin:GetRule",
        "rbin:ListRules",
        "rbin:ListTagsForResource",
        "rds:Describe*",
        "rds:Download*",
        "rds:List*",
        "redshift-serverless:GetCustomDomainAssociation",
        "redshift-serverless:GetEndpointAccess",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetRecoveryPoint",
        "redshift-serverless:GetResourcePolicy",
        "redshift-serverless:GetScheduledAction",
        "redshift-serverless:GetSnapshot",
        "redshift-serverless:GetTableRestoreStatus",
        "redshift-serverless:GetUsageLimit",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:ListCustomDomainAssociations",
```

```
        "redshift-serverless:ListEndpointAccess",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListRecoveryPoints",
        "redshift-serverless:ListScheduledActions",
        "redshift-serverless:ListSnapshotCopyConfigurations",
        "redshift-serverless:ListSnapshots",
        "redshift-serverless:ListTableRestoreStatus",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:ListUsageLimits",
        "redshift-serverless:ListWorkgroups",
        "redshift:Describe*",
        "redshift:GetReservedNodeExchangeOfferings",
        "redshift:ListRecommendations",
        "redshift:View*",
        "refactor-spaces:GetApplication",
        "refactor-spaces:GetEnvironment",
        "refactor-spaces:GetResourcePolicy",
        "refactor-spaces:GetRoute",
        "refactor-spaces:GetService",
        "refactor-spaces:ListApplications",
        "refactor-spaces:ListEnvironmentVpcs",
        "refactor-spaces:ListEnvironments",
        "refactor-spaces:ListRoutes",
        "refactor-spaces:ListServices",
        "refactor-spaces:ListTagsForResource",
        "rekognition:CompareFaces",
        "rekognition:DescribeDataset",
        "rekognition:DescribeProjectVersions",
        "rekognition:DescribeProjects",
        "rekognition:DescribeStreamProcessor",
        "rekognition:Detect*",
        "rekognition:GetCelebrityInfo",
        "rekognition:GetCelebrityRecognition",
        "rekognition:GetContentModeration",
        "rekognition:GetFaceDetection",
        "rekognition:GetFaceSearch",
        "rekognition:GetLabelDetection",
        "rekognition:GetPersonTracking",
        "rekognition:GetSegmentDetection",
        "rekognition:GetTextDetection",
        "rekognition:List*",
        "rekognition:RecognizeCelebrities",
        "rekognition:Search*",
        "resiliencehub:DescribeApp",
```

```
        "resiliencehub:DescribeAppAssessment",
        "resiliencehub:DescribeAppVersion",
        "resiliencehub:DescribeAppVersionAppComponent",
        "resiliencehub:DescribeAppVersionResource",
        "resiliencehub:DescribeAppVersionResourcesResolutionStatus",
        "resiliencehub:DescribeAppVersionTemplate",
        "resiliencehub:DescribeDraftAppVersionResourcesImportStatus",
        "resiliencehub:DescribeMetricsExport",
        "resiliencehub:DescribeResiliencyPolicy",
        "resiliencehub:DescribeResourceGroupingRecommendationTask",
        "resiliencehub:ListAlarmRecommendations",
        "resiliencehub:ListAppAssessmentComplianceDrifts",
        "resiliencehub:ListAppAssessmentResourceDrifts",
        "resiliencehub:ListAppAssessments",
        "resiliencehub:ListAppComponentCompliances",
        "resiliencehub:ListAppComponentRecommendations",
        "resiliencehub:ListAppInputSources",
        "resiliencehub:ListAppVersionAppComponents",
        "resiliencehub:ListAppVersionResourceMappings",
        "resiliencehub:ListAppVersionResources",
        "resiliencehub:ListAppVersions",
        "resiliencehub:ListApps",
        "resiliencehub:ListMetrics",
        "resiliencehub:ListRecommendationTemplates",
        "resiliencehub:ListResiliencyPolicies",
        "resiliencehub:ListResourceGroupingRecommendations",
        "resiliencehub:ListSopRecommendations",
        "resiliencehub:ListSuggestedResiliencyPolicies",
        "resiliencehub:ListTagsForResource",
        "resiliencehub:ListTestRecommendations",
        "resiliencehub:ListUnsupportedAppVersionResources",
        "resource-explorer-2:BatchGetView",
        "resource-explorer-2:GetAccountLevelServiceConfiguration",
        "resource-explorer-2:GetDefaultView",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:GetManagedView",
        "resource-explorer-2:GetResourceExplorerSetup",
        "resource-explorer-2:GetServiceIndex",
        "resource-explorer-2:GetServiceView",
        "resource-explorer-2:GetView",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListIndexesForMembers",
        "resource-explorer-2:ListManagedViews",
        "resource-explorer-2:ListServiceIndexes",
```

```
        "resource-explorer-2:ListServiceViews",
        "resource-explorer-2:ListStreamingAccessForServices",
        "resource-explorer-2:ListSupportedResourceTypes",
        "resource-explorer-2:ListTagsForResource",
        "resource-explorer-2:ListViews",
        "resource-explorer-2:Search",
        "resource-groups:Get*",
        "resource-groups:List*",
        "resource-groups:Search*",
        "robomaker:BatchDescribe*",
        "robomaker:Describe*",
        "robomaker:Get*",
        "robomaker:List*",
        "rolesanywhere:GetCrl",
        "rolesanywhere:GetProfile",
        "rolesanywhere:GetSubject",
        "rolesanywhere:GetTrustAnchor",
        "rolesanywhere:ListCrls",
        "rolesanywhere:ListProfiles",
        "rolesanywhere:ListSubjects",
        "rolesanywhere:ListTagsForResource",
        "rolesanywhere:ListTrustAnchors",
        "route53-recovery-cluster:Get*",
        "route53-recovery-cluster:ListRoutingControls",
        "route53-recovery-control-config:Describe*",
        "route53-recovery-control-config:GetResourcePolicy",
        "route53-recovery-control-config:List*",
        "route53-recovery-readiness:Get*",
        "route53-recovery-readiness:List*",
        "route53:Get*",
        "route53:List*",
        "route53:Test*",
        "route53domains:Check*",
        "route53domains:Get*",
        "route53domains:List*",
        "route53domains:View*",
        "route53profiles:GetProfile",
        "route53profiles:GetProfileAssociation",
        "route53profiles:GetProfileResourceAssociation",
        "route53profiles:ListProfileAssociations",
        "route53profiles:ListProfileResourceAssociations",
        "route53profiles:ListProfiles",
        "route53profiles:ListTagsForResource",
        "route53resolver:Get*",
```

```
        "route53resolver:List*",
        "rum:GetAppMonitor",
        "rum:GetAppMonitorData",
        "rum:ListAppMonitors",
        "s3-object-lambda:GetObject",
        "s3-object-lambda:GetObjectAcl",
        "s3-object-lambda:GetObjectLegalHold",
        "s3-object-lambda:GetObjectRetention",
        "s3-object-lambda:GetObjectTagging",
        "s3-object-lambda:GetObjectVersion",
        "s3-object-lambda:GetObjectVersionAcl",
        "s3-object-lambda:GetObjectVersionTagging",
        "s3-object-lambda:ListBucket",
        "s3-object-lambda:ListBucketMultipartUploads",
        "s3-object-lambda:ListBucketVersions",
        "s3-object-lambda:ListMultipartUploadParts",
        "s3-outposts:GetAccessPoint",
        "s3-outposts:GetAccessPointPolicy",
        "s3-outposts:GetBucket",
        "s3-outposts:GetBucketPolicy",
        "s3-outposts:GetBucketTagging",
        "s3-outposts:GetBucketVersioning",
        "s3-outposts:GetLifecycleConfiguration",
        "s3-outposts:GetObject",
        "s3-outposts:GetObjectTagging",
        "s3-outposts:GetObjectVersion",
        "s3-outposts:GetObjectVersionForReplication",
        "s3-outposts:GetObjectVersionTagging",
        "s3-outposts:GetReplicationConfiguration",
        "s3-outposts:ListAccessPoints",
        "s3-outposts:ListBucket",
        "s3-outposts:ListBucketMultipartUploads",
        "s3-outposts:ListBucketVersions",
        "s3-outposts:ListEndpoints",
        "s3-outposts:ListMultipartUploadParts",
        "s3-outposts:ListOutpostsWithS3",
        "s3-outposts:ListRegionalBuckets",
        "s3-outposts:ListSharedEndpoints",
        "s3:DescribeJob",
        "s3:Get*",
        "s3:List*",
        "s3vectors:GetIndex",
        "s3vectors:GetVectorBucket",
        "s3vectors:GetVectorBucketPolicy",
```

```
        "s3vectors:GetVectors",
        "s3vectors:ListIndexes",
        "s3vectors:ListVectorBuckets",
        "s3vectors:ListVectors",
        "s3vectors:QueryVectors",
        "s3tables:GetTable",
        "s3tables:GetTableBucket",
        "s3tables:GetTableBucketEncryption",
        "s3tables:GetTableBucketMaintenanceConfiguration",
        "s3tables:GetTableBucketPolicy",
        "s3tables:GetTableBucketReplication",
        "s3tables:GetTableBucketStorageClass",
        "s3tables:GetTableData",
        "s3tables:GetTableEncryption",
        "s3tables:GetTableMaintenanceConfiguration",
        "s3tables:GetTableMaintenanceJobStatus",
        "s3tables:GetTableMetadataLocation",
        "s3tables:GetTablePolicy",
        "s3tables:GetTableRecordExpirationConfiguration",
        "s3tables:GetTableRecordExpirationJobStatus",
        "s3tables:GetTableReplication",
        "s3tables:GetTableReplicationStatus",
        "s3tables:GetTableStorageClass",
        "s3tables:ListNamespaces",
        "s3tables:ListTableBuckets",
        "s3tables:ListTables",
        "s3tables:ListTagsForResource",
        "s3tables:GetNamespace",
        "sagemaker:Describe*",
        "sagemaker:GetSearchSuggestions",
        "sagemaker:List*",
        "sagemaker:Search",
        "savingsplans:DescribeSavingsPlanRates",
        "savingsplans:DescribeSavingsPlans",
        "savingsplans:DescribeSavingsPlansOfferingRates",
        "savingsplans:DescribeSavingsPlansOfferings",
        "savingsplans:ListTagsForResource",
        "scheduler:GetSchedule",
        "scheduler:GetScheduleGroup",
        "scheduler:ListScheduleGroups",
        "scheduler:ListSchedules",
        "scheduler:ListTagsForResource",
        "schemas:Describe*",
        "schemas:Get*",
```

```
        "schemas:List*",
        "schemas:Search*",
        "sdb:Get*",
        "sdb:List*",
        "sdb:Select*",
        "secretsmanager:Describe*",
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:List*",
        "securityhub:BatchGetAutomationRules",
        "securityhub:BatchGetConfigurationPolicyAssociations",
        "securityhub:BatchGetControlEvaluations",
        "securityhub:BatchGetSecurityControls",
        "securityhub:BatchGetStandardsControlAssociations",
        "securityhub:Describe*",
        "securityhub:Get*",
        "securityhub:List*",
        "securitylake:GetDataLakeExceptionSubscription",
        "securitylake:GetDataLakeOrganizationConfiguration",
        "securitylake:GetDataLakeSources",
        "securitylake:GetSubscriber",
        "securitylake:ListDataLakeExceptions",
        "securitylake:ListDataLakes",
        "securitylake:ListLogSources",
        "securitylake:ListSubscribers",
        "securitylake:ListTagsForResource",
        "serverlessrepo:Get*",
        "serverlessrepo:List*",
        "serverlessrepo:SearchApplications",
        "servicecatalog:Describe*",
        "servicecatalog:GetApplication",
        "servicecatalog:GetAttributeGroup",
        "servicecatalog:List*",
        "servicecatalog:Scan*",
        "servicecatalog:Search*",
        "servicediscovery:DiscoverInstances",
        "servicediscovery:DiscoverInstancesRevision",
        "servicediscovery:Get*",
        "servicediscovery:List*",
        "servicequotas:GetAWSDefaultServiceQuota",
        "servicequotas:GetAssociationForServiceQuotaTemplate",
        "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:DescribeOptOutLists",
        "sms-voice:DescribeOptedOutNumbers",
        "sms-voice:DescribePhoneNumbers",
        "sms-voice:DescribePools",
        "sms-voice:DescribeProtectConfigurations",
        "sms-voice:DescribeRegistrationAttachments",
        "sms-voice:DescribeRegistrationFieldDefinitions",
        "sms-voice:DescribeRegistrationFieldValues",
        "sms-voice:DescribeRegistrations",
        "sms-voice:DescribeRegistrationSectionDefinitions",
        "sms-voice:DescribeRegistrationTypeDefinitions",
        "sms-voice:DescribeRegistrationVersions",
        "sms-voice:DescribeSenderIds",
        "sms-voice:DescribeSpendLimits",
        "sms-voice:DescribeVerifiedDestinationNumbers",
        "sms-voice:ListPoolOriginationIdentities",
        "sms-voice:ListTagsForResource",
        "snowball:Describe*",
        "snowball:Get*",
```

```
        "snowball:List*",
        "sns:Check*",
        "sns:Get*",
        "sns:List*",
        "sqs:Get*",
        "sqs:List*",
        "sqs:Receive*",
        "ssm-contacts:DescribeEngagement",
        "ssm-contacts:DescribePage",
        "ssm-contacts:GetContact",
        "ssm-contacts:GetContactChannel",
        "ssm-contacts:ListContactChannels",
        "ssm-contacts:ListContacts",
        "ssm-contacts:ListEngagements",
        "ssm-contacts:ListPageReceipts",
        "ssm-contacts:ListPagesByContact",
        "ssm-contacts:ListPagesByEngagement",
        "ssm-incidents:GetIncidentRecord",
        "ssm-incidents:GetReplicationSet",
        "ssm-incidents:GetResourcePolicies",
        "ssm-incidents:GetResponsePlan",
        "ssm-incidents:GetTimelineEvent",
        "ssm-incidents:ListIncidentRecords",
        "ssm-incidents:ListRelatedItems",
        "ssm-incidents:ListReplicationSets",
        "ssm-incidents:ListResponsePlans",
        "ssm-incidents:ListTagsForResource",
        "ssm-incidents:ListTimelineEvents",
        "ssm-quicksetup:GetConfiguration",
        "ssm-quicksetup:GetConfigurationManager",
        "ssm-quicksetup:GetServiceSettings",
        "ssm-quicksetup:ListConfigurationManagers",
        "ssm-quicksetup:ListConfigurations",
        "ssm-quicksetup:ListQuickSetupTypes",
        "ssm-quicksetup:ListTagsForResource",
        "ssm-sap:GetApplication",
        "ssm-sap:GetComponent",
        "ssm-sap:GetConfigurationCheckOperation",
        "ssm-sap:GetDatabase",
        "ssm-sap:GetOperation",
        "ssm-sap:GetResourcePermission",
        "ssm-sap:ListApplications",
        "ssm-sap:ListComponents",
        "ssm-sap:ListConfigurationCheckDefinitions",
```

```
        "ssm-sap:ListConfigurationCheckOperations",
        "ssm-sap:ListDatabases",
        "ssm-sap:ListOperationEvents",
        "ssm-sap:ListOperations",
        "ssm-sap:ListSubCheckResults",
        "ssm-sap:ListSubCheckRuleResults",
        "ssm-sap:ListTagsForResource",
        "ssm:Describe*",
        "ssm:Get*",
        "ssm:List*",
        "sso-directory:Describe*",
        "sso-directory:List*",
        "sso-directory:Search*",
        "sso:Describe*",
        "sso:Get*",
        "sso:List*",
        "states:Describe*",
        "states:GetExecutionHistory",
        "states:List*",
        "states:ValidateStateMachineDefinition",
        "storagegateway:Describe*",
        "storagegateway:List*",
        "sts:GetAccessKeyInfo",
        "sts:GetCallerIdentity",
        "sts:GetSessionToken",
        "support:DescribeAttachment",
        "support:DescribeCaseAttributes",
        "support:DescribeCases",
        "support:DescribeCommunication",
        "support:DescribeCommunications",
        "support:DescribeCreateCaseOptions",
        "support:DescribeIssueTypes",
        "support:DescribeServices",
        "support:DescribeSeverityLevels",
        "support:DescribeSupportLevel",
        "support:DescribeSupportedLanguages",
        "support:DescribeTrustedAdvisorCheckRefreshStatuses",
        "support:DescribeTrustedAdvisorCheckResult",
        "support:DescribeTrustedAdvisorCheckSummaries",
        "support:DescribeTrustedAdvisorChecks",
        "support:SearchForCases",
        "supportplans:GetSupportPlan",
        "supportplans:GetSupportPlanUpdateStatus",
        "supportplans:ListSupportPlanModifiers",
```

```
        "sustainability:GetCarbonFootprintSummary",
        "swf:Count*",
        "swf:Describe*",
        "swf:Get*",
        "swf:List*",
        "synthetics:Describe*",
        "synthetics:Get*",
        "synthetics:List*",
        "tag:DescribeReportCreation",
        "tag:Get*",
        "tax:GetExemptions",
        "tax:GetTaxInheritance",
        "tax:GetTaxInterview",
        "tax:GetTaxRegistration",
        "tax:GetTaxRegistrationDocument",
        "tax:ListTaxRegistrations",
        "timestream:DescribeBatchLoadTask",
        "timestream:DescribeDatabase",
        "timestream:DescribeEndpoints",
        "timestream:DescribeTable",
        "timestream:ListBatchLoadTasks",
        "timestream:ListDatabases",
        "timestream:ListMeasures",
        "timestream:ListTables",
        "timestream:ListTagsForResource",
        "tnb:GetSolFunctionInstance",
        "tnb:GetSolFunctionPackage",
        "tnb:GetSolFunctionPackageContent",
        "tnb:GetSolFunctionPackageDescriptor",
        "tnb:GetSolNetworkInstance",
        "tnb:GetSolNetworkOperation",
        "tnb:GetSolNetworkPackage",
        "tnb:GetSolNetworkPackageContent",
        "tnb:GetSolNetworkPackageDescriptor",
        "tnb:ListSolFunctionInstances",
        "tnb:ListSolFunctionPackages",
        "tnb:ListSolNetworkInstances",
        "tnb:ListSolNetworkOperations",
        "tnb:ListSolNetworkPackages",
        "tnb:ListTagsForResource",
        "transcribe:Get*",
        "transcribe:List*",
        "transfer:Describe*",
        "transfer:List*",
```

```
        "transfer:TestIdentityProvider",
        "translate:DescribeTextTranslationJob",
        "translate:GetParallelData",
        "translate:GetTerminology",
        "translate:ListParallelData",
        "translate:ListTerminologies",
        "translate:ListTextTranslationJobs",
        "trustedadvisor:Describe*",
        "trustedadvisor:GetOrganizationRecommendation",
        "trustedadvisor:GetRecommendation",
        "trustedadvisor:ListChecks",
        "trustedadvisor:ListOrganizationRecommendationAccounts",
        "trustedadvisor:ListOrganizationRecommendationResources",
        "trustedadvisor:ListOrganizationRecommendations",
        "trustedadvisor:ListRecommendationResources",
        "trustedadvisor:ListRecommendations",
        "user-subscriptions:ListApplicationClaims",
        "user-subscriptions:ListClaims",
        "user-subscriptions:ListUserSubscriptions",
        "uxc:GetAccountColor",
        "verifiedpermissions:GetIdentitySource",
        "verifiedpermissions:GetPolicy",
        "verifiedpermissions:GetPolicyStore",
        "verifiedpermissions:GetPolicyTemplate",
        "verifiedpermissions:GetSchema",
        "verifiedpermissions:IsAuthorized",
        "verifiedpermissions:IsAuthorizedWithToken",
        "verifiedpermissions:ListIdentitySources",
        "verifiedpermissions:ListPolicies",
        "verifiedpermissions:ListPolicyStores",
        "verifiedpermissions:ListPolicyTemplates",
        "vpc-lattice:GetAccessLogSubscription",
        "vpc-lattice:GetAuthPolicy",
        "vpc-lattice:GetListener",
        "vpc-lattice:GetResourceConfiguration",
        "vpc-lattice:GetResourceGateway",
        "vpc-lattice:GetResourcePolicy",
        "vpc-lattice:GetRule",
        "vpc-lattice:GetService",
        "vpc-lattice:GetServiceNetwork",
        "vpc-lattice:GetServiceNetworkResourceAssociation",
        "vpc-lattice:GetServiceNetworkServiceAssociation",
        "vpc-lattice:GetServiceNetworkVpcAssociation",
        "vpc-lattice:GetTargetGroup",
```

```
        "vpc-lattice:ListAccessLogSubscriptions",
        "vpc-lattice:ListListeners",
        "vpc-lattice:ListResourceConfigurations",
        "vpc-lattice:ListResourceEndpointAssociations",
        "vpc-lattice:ListResourceGateways",
        "vpc-lattice:ListRules",
        "vpc-lattice:ListServiceNetworkResourceAssociations",
        "vpc-lattice:ListServiceNetworkServiceAssociations",
        "vpc-lattice:ListServiceNetworkVpcAssociations",
        "vpc-lattice:ListServiceNetworks",
        "vpc-lattice:ListServiceNetworkVpcEndpointAssociations",
        "vpc-lattice:ListServices",
        "vpc-lattice:ListTagsForResource",
        "vpc-lattice:ListTargetGroups",
        "vpc-lattice:ListTargets",
        "waf-regional:Get*",
        "waf-regional:List*",
        "waf:Get*",
        "waf:List*",
        "wafv2:CheckCapacity",
        "wafv2:Describe*",
        "wafv2:Get*",
        "wafv2:List*",
        "wellarchitected:ExportLens",
        "wellarchitected:GetAnswer",
        "wellarchitected:GetConsolidatedReport",
        "wellarchitected:GetLens",
        "wellarchitected:GetLensReview",
        "wellarchitected:GetLensReviewReport",
        "wellarchitected:GetLensVersionDifference",
        "wellarchitected:GetMilestone",
        "wellarchitected:GetProfile",
        "wellarchitected:GetProfileTemplate",
        "wellarchitected:GetReviewTemplate",
        "wellarchitected:GetReviewTemplateAnswer",
        "wellarchitected:GetReviewTemplateLensReview",
        "wellarchitected:GetWorkload",
        "wellarchitected:List*",
        "workdocs:CheckAlias",
        "workdocs:Describe*",
        "workdocs:Get*",
        "workmail:Describe*",
        "workmail:Get*",
        "workmail:List*",
```

```
        "workmail:Search*",
        "workspaces-web:GetBrowserSettings",
        "workspaces-web:GetIdentityProvider",
        "workspaces-web:GetNetworkSettings",
        "workspaces-web:GetPortal",
        "workspaces-web:GetPortalServiceProviderMetadata",
        "workspaces-web:GetTrustStore",
        "workspaces-web:GetUserAccessLoggingSettings",
        "workspaces-web:GetUserSettings",
        "workspaces-web:ListBrowserSettings",
        "workspaces-web:ListIdentityProviders",
        "workspaces-web:ListNetworkSettings",
        "workspaces-web:ListPortals",
        "workspaces-web:ListTagsForResource",
        "workspaces-web:ListTrustStores",
        "workspaces-web:ListUserAccessLoggingSettings",
        "workspaces-web:ListUserSettings",
        "workspaces:Describe*",
        "xray:BatchGet*",
        "xray:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

ResourceGroupsandTagEditorFullAccess

説明: Resource Groups およびタグエディタへのフルアクセスを提供します。

`ResourceGroupsandTagEditorFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに ResourceGroupsandTagEditorFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:39 UTC
- 編集日時: 2023 年 8 月 10 日 13:29 UTC
- ARN: arn:aws:iam::aws:policy/ResourceGroupsandTagEditorFullAccess

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
```

```
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

ResourceGroupsandTagEditorReadOnlyAccess

説明: Resource Groups およびタグエディターを使用するためのアクセスを提供しますが、タグエディターを経由したタグの編集は許可しません。

`ResourceGroupsandTagEditorReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `ResourceGroupsandTagEditorReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:39 UTC
- 編集日時: 2023 年 8 月 10 日 13:42 UTC
- ARN: `arn:aws:iam::aws:policy/ResourceGroupsandTagEditorReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

ResourceGroupsServiceRolePolicy

説明: Resource Groups が AWS リソースを所有する AWS サービスをクエリして、グループをup-to-dateに保つことを許可します。

`ResourceGroupsServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 1 月 5 日 16:57 UTC
- 編集日時: 2023 年 1 月 5 日 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ResourceGroupsServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

ResourceGroupsTaggingAPITagUntagSupportedResources

説明: リソースグループタグ付け API でサポートされているすべてのリソースにタグを付けたり、タグを解除することを許可します。また、このポリシーは、リソースグループタグ付け API を使用して、タグ付けされた、または以前にタグ付けされたすべてのリソースを取得するのに必要な許可を付与します。

`ResourceGroupsTaggingAPITagUntagSupportedResources` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `ResourceGroupsTaggingAPITagUntagSupportedResources` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 10 月 11 日 11:11 UTC
- 編集日時: 2024 年 12 月 11 日 17:51 UTC
- ARN: `arn:aws:iam::aws:policy/ResourceGroupsTaggingAPITagUntagSupportedResources`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:TagResource",
        "a4b:UntagResource",
        "access-analyzer:TagResource",
        "access-analyzer:UntagResource",
        "acm-pca:TagCertificateAuthority",
        "acm-pca:UntagCertificateAuthority",
        "acm:AddTagsToCertificate",
        "acm:RemoveTagsFromCertificate",
        "amplify:TagResource",
        "amplify:UntagResource",
        "appconfig:TagResource",
        "appconfig:UntagResource",
        "appflow:TagResource",
        "appflow:UntagResource",
        "appmesh:TagResource",
        "appmesh:UntagResource",
        "appstream:TagResource",
        "appstream:UntagResource",
        "appsync:TagResource",
        "appsync:UntagResource",
        "athena:TagResource",
        "athena:UntagResource",
        "auditmanager:TagResource",
        "auditmanager:UntagResource",
        "autoscaling:CreateOrUpdateTags",
        "autoscaling:DeleteTags",
        "backup:TagResource",
        "backup:UntagResource",
        "batch:TagResource",
        "batch:UntagResource",
        "braket:TagResource",
        "braket:UntagResource",
        "cassandra:TagResource",
        "cassandra:UntagResource",
        "chime:TagResource",
```

```
        "chime:UntagResource",
        "cloud9:TagResource",
        "cloud9:UntagResource",
        "clouddirectory:TagResource",
        "clouddirectory:UntagResource",
        "cloudfront:TagResource",
        "cloudfront:UntagResource",
        "cloudhsm:TagResource",
        "cloudhsm:UntagResource",
        "cloudtrail:AddTags",
        "cloudtrail:RemoveTags",
        "cloudwatch:TagResource",
        "cloudwatch:UntagResource",
        "codeartifact:TagResource",
        "codeartifact:UntagResource",
        "codecommit:TagResource",
        "codecommit:UntagResource",
        "codedeploy:AddTagsToOnPremisesInstances",
        "codedeploy:RemoveTagsFromOnPremisesInstances",
        "codedeploy:TagResource",
        "codedeploy:UntagResource",
        "codeguru-profiler:TagResource",
        "codeguru-profiler:UntagResource",
        "codepipeline:TagResource",
        "codepipeline:UntagResource",
        "codestar-connections:TagResource",
        "codestar-connections:UntagResource",
        "codestar:TagProject",
        "codestar:UntagProject",
        "cognito-identity:TagResource",
        "cognito-identity:UntagResource",
        "cognito-idp:TagResource",
        "cognito-idp:UntagResource",
        "comprehend:TagResource",
        "comprehend:UntagResource",
        "config:TagResource",
        "config:UntagResource",
        "connect:TagResource",
        "connect:UntagResource",
        "dataexchange:TagResource",
        "dataexchange:UntagResource",
        "datapipeline:AddTags",
        "datapipeline:RemoveTags",
        "datasync:TagResource",
```

```
        "datasync:UntagResource",
        "deepcomposer:TagResource",
        "deepcomposer:UntagResource",
        "detective:TagResource",
        "detective:UntagResource",
        "devicefarm:TagResource",
        "devicefarm:UntagResource",
        "directconnect:TagResource",
        "directconnect:UntagResource",
        "dlm:TagResource",
        "dlm:UntagResource",
        "dms:AddTagsToResource",
        "dms:RemoveTagsFromResource",
        "dynamodb:TagResource",
        "dynamodb:UntagResource",
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "ecr:TagResource",
        "ecr:UntagResource",
        "ecs:TagResource",
        "ecs:UntagResource",
        "eks:TagResource",
        "eks:UntagResource",
        "elastic-inference:TagResource",
        "elastic-inference:UntagResource",
        "elasticache:AddTagsToResource",
        "elasticache:RemoveTagsFromResource",
        "elasticbeanstalk:UpdateTagsForResource",
        "elasticfilesystem:CreateTags",
        "elasticfilesystem:DeleteTags",
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:RemoveTags",
        "elasticmapreduce:AddTags",
        "elasticmapreduce:RemoveTags",
        "emr-containers:TagResource",
        "emr-containers:UntagResource",
        "es:AddTags",
        "es:RemoveTags",
        "events:TagResource",
        "events:UntagResource",
        "firehose:TagDeliveryStream",
        "firehose:UntagDeliveryStream",
        "fms:TagResource",
        "fms:UntagResource",
```

```
        "forecast:TagResource",
        "forecast:UntagResource",
        "frauddetector:TagResource",
        "frauddetector:UntagResource",
        "fsx:TagResource",
        "fsx:UntagResource",
        "gamelift:TagResource",
        "gamelift:UntagResource",
        "glacier:AddTagsToVault",
        "glacier:RemoveTagsFromVault",
        "globalaccelerator:TagResource",
        "globalaccelerator:UntagResource",
        "glue:TagResource",
        "glue:UntagResource",
        "greengrass:TagResource",
        "greengrass:UntagResource",
        "groundstation:TagResource",
        "groundstation:UntagResource",
        "guardduty:TagResource",
        "guardduty:UntagResource",
        "iam:TagInstanceProfile",
        "iam:TagMFADevice",
        "iam:TagOpenIDConnectProvider",
        "iam:TagPolicy",
        "iam:TagRole",
        "iam:TagSAMLProvider",
        "iam:TagServerCertificate",
        "iam:TagUser",
        "iam:UntagInstanceProfile",
        "iam:UntagMFADevice",
        "iam:UntagOpenIDConnectProvider",
        "iam:UntagPolicy",
        "iam:UntagRole",
        "iam:UntagSAMLProvider",
        "iam:UntagServerCertificate",
        "iam:UntagUser",
        "imagebuilder:TagResource",
        "imagebuilder:UntagResource",
        "inspector:ListTagsForResource",
        "inspector:SetTagsForResource",
        "iot1click:TagResource",
        "iot1click:UntagResource",
        "iot:TagResource",
        "iot:UntagResource",
```

```
        "iotanalytics:TagResource",
        "iotanalytics:UntagResource",
        "iotdeviceadvisor:TagResource",
        "iotdeviceadvisor:UntagResource",
        "iotevents:TagResource",
        "iotevents:UntagResource",
        "iotfleethub:TagResource",
        "iotfleethub:UntagResource",
        "iotsitewise:TagResource",
        "iotsitewise:UntagResource",
        "iottwinmaker:TagResource",
        "iottwinmaker:UntagResource",
        "iotwireless:TagResource",
        "iotwireless:UntagResource",
        "ivs:TagResource",
        "ivs:UntagResource",
        "kafka:TagResource",
        "kafka:UntagResource",
        "kendra:TagResource",
        "kendra:UntagResource",
        "kinesis:AddTagsToStream",
        "kinesis:RemoveTagsFromStream",
        "kinesisanalytics:TagResource",
        "kinesisanalytics:UntagResource",
        "kms:TagResource",
        "kms:UntagResource",
        "lambda:TagResource",
        "lambda:UntagResource",
        "lex:TagResource",
        "lex:UntagResource",
        "license-manager:TagResource",
        "license-manager:UntagResource",
        "lightsail:TagResource",
        "lightsail:UntagResource",
        "logs:TagLogGroup",
        "logs:TagResource",
        "logs:UntagLogGroup",
        "logs:UntagResource",
        "lookoutequipment:TagResource",
        "lookoutequipment:UntagResource",
        "machinelearning:AddTags",
        "machinelearning:DeleteTags",
        "macie2:TagResource",
        "macie2:UntagResource",
```

```
        "managedblockchain:TagResource",
        "managedblockchain:UntagResource",
        "mediaconnect:TagResource",
        "mediaconnect:UntagResource",
        "mediaconvert:TagResource",
        "mediaconvert:UntagResource",
        "medialive:CreateTags",
        "medialive:DeleteTags",
        "mediapackage-vod:TagResource",
        "mediapackage-vod:UntagResource",
        "mediapackage:TagResource",
        "mediapackage:UntagResource",
        "mediatailor:TagResource",
        "mediatailor:UntagResource",
        "mobiletargeting:TagResource",
        "mobiletargeting:UntagResource",
        "mq:CreateTags",
        "mq:DeleteTags",
        "neptune-graph:TagResource",
        "neptune-graph:UntagResource",
        "network-firewall:TagResource",
        "network-firewall:UntagResource",
        "networkmanager:TagResource",
        "networkmanager:UntagResource",
        "opsworks-cm:TagResource",
        "opsworks-cm:UntagResource",
        "opsworks:TagResource",
        "opsworks:UntagResource",
        "organizations:TagResource",
        "organizations:UntagResource",
        "outposts:TagResource",
        "outposts:UntagResource",
        "qldb:TagResource",
        "qldb:UntagResource",
        "quicksight:TagResource",
        "quicksight:UntagResource",
        "ram:TagResource",
        "ram:UntagResource",
        "rds:AddTagsToResource",
        "rds:RemoveTagsFromResource",
        "redshift:CreateTags",
        "redshift:DeleteTags",
        "resource-explorer-2:TagResource",
        "resource-explorer-2:UntagResource",
```

```
        "resource-groups:Tag",
        "resource-groups:Untag",
        "robomaker:TagResource",
        "robomaker:UntagResource",
        "route53:ChangeTagsForResource",
        "route53domains:DeleteTagsForDomain",
        "route53domains:UpdateTagsForDomain",
        "route53resolver:TagResource",
        "route53resolver:UntagResource",
        "s3:GetBucketTagging",
        "s3:GetJobTagging",
        "s3:GetObjectTagging",
        "s3:GetObjectVersionTagging",
        "s3:GetStorageLensConfigurationTagging",
        "s3:DeleteJobTagging",
        "s3:DeleteObjectTagging",
        "s3:DeleteObjectVersionTagging",
        "s3:PutBucketTagging",
        "s3:PutJobTagging",
        "s3:PutObjectTagging",
        "s3:PutObjectVersionTagging",
        "s3:PutStorageLensConfigurationTagging",
        "s3:DeleteStorageLensConfigurationTagging",
        "s3:TagResource",
        "s3:UntagResource",
        "sagemaker:AddTags",
        "sagemaker:DeleteTags",
        "savingsplans:TagResource",
        "savingsplans:UntagResource",
        "schemas:TagResource",
        "schemas:UntagResource",
        "secretsmanager:TagResource",
        "secretsmanager:UntagResource",
        "securityhub:TagResource",
        "securityhub:UntagResource",
        "servicediscovery:TagResource",
        "servicediscovery:UntagResource",
        "servicequotas:TagResource",
        "servicequotas:UntagResource",
        "ses:TagResource",
        "ses:UntagResource",
        "sns:TagResource",
        "sns:UntagResource",
        "sqs:TagQueue",
```

```
        "sqs:UntagQueue",
        "ssm:AddTagsToResource",
        "ssm:RemoveTagsFromResource",
        "states:TagResource",
        "states:UntagResource",
        "storagegateway:AddTagsToResource",
        "storagegateway:RemoveTagsFromResource",
        "swf:TagResource",
        "swf:UntagResource",
        "synthetics:TagResource",
        "synthetics:UntagResource",
        "tag:GetResources",
        "tag:TagResources",
        "tag:UntagResources",
        "transfer:TagResource",
        "transfer:UntagResource",
        "waf-regional:TagResource",
        "waf-regional:UntagResource",
        "waf:TagResource",
        "waf:UntagResource",
        "wafv2:TagResource",
        "wafv2:UntagResource",
        "worklink:TagResource",
        "worklink:UntagResource",
        "workmail:TagResource",
        "workmail:UntagResource",
        "workspaces:CreateTags",
        "workspaces:DeleteTags",
        "xray:TagResource",
        "xray:UntagResource",
        "kinesisvideo:TagResource",
        "kinesisvideo:UntagResource",
        "redshift-serverless:TagResource",
        "redshift-serverless:UntagResource",
        "route53-recovery-control-config:TagResource",
        "route53-recovery-control-config:UntagResource",
        "route53-recovery-readiness:TagResource",
        "route53-recovery-readiness:UntagResource",
        "ssm-contacts:TagResource",
        "ssm-contacts:UntagResource",
        "ssm-incidents:TagResource",
        "ssm-incidents:UntagResource",
        "vpc-lattice:TagResource",
        "vpc-lattice:UntagResource",
```

```
        "workspaces-web:TagResource",
        "workspaces-web:UntagResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

ROSAAmazonEBSCSIDriverOperatorPolicy

説明: OpenShift Amazon EBS Container Storage Interface (CSI) ドライバーオペレーターが Red Hat OpenShift Service on AWS (ROSA) クラスターに Amazon EBS CSI ドライバーをインストールして維持できるようにします。Amazon EBS CSI ドライバーは、ROSA クラスターが永続ボリューム用 Amazon EBS ボリュームのライフサイクルを管理できるようにします。

`ROSAAmazonEBSCSIDriverOperatorPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `ROSAAmazonEBSCSIDriverOperatorPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 4 月 20 日 22:36 UTC
- 編集日時: 2025 年 1 月 22 日 00:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAAmazonEBSCSIDriverOperatorPolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshots",
        "ec2:DescribeTags",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:DeleteVolume",
        "ec2:ModifyVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateVolumeFromSnapshot",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*"
      ]
    },
    {
      "Sid" : "CreateSnapshotResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotRequestTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateVolume",
            "CreateSnapshot"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

ROSACloudNetworkConfigOperatorPolicy

説明: OpenShift Cloud Network Config Controller Operator が、Red Hat OpenShift Service on AWS (ROSA) クラスターネットワーキングオーバーレイで使用するネットワークリソースをプロビジョニングおよび管理できるようにします。OpenShift クラウドネットワークオペレーターは、CustomResourceDefinitions を介してネットワークプラグインに代わって AWS APIs とインターフェイスします。 CustomResourceDefinitions オペレーターはこれらのポリシー許可を使用し、ROSA クラスターの一部として Amazon EC2 インスタンスのプライベート IP アドレスを管理します。

`ROSACloudNetworkConfigOperatorPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `ROSACloudNetworkConfigOperatorPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 4 月 20 日 22:34 UTC
- 編集日時: 2023 年 4 月 20 日 22:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSACloudNetworkConfigOperatorPolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

ROSAControlPlaneOperatorPolicy

説明: Red Hat OpenShift Service on AWS (ROSA) コントロールプレーンが ROSA クラスターの Amazon EC2 および Amazon Route 53 リソースを管理できるようにします。

`ROSAControlPlaneOperatorPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `ROSAControlPlaneOperatorPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 4 月 24 日 23:02 UTC
- 編集日時: 2025 年 4 月 10 日 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAControlPlaneOperatorPolicy`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

ROSAImageRegistryOperatorPolicy

説明: OpenShift Image Registry Operator が、Red Hat OpenShift Service on AWS (ROSA) クラスター内イメージレジストリで使用する Amazon S3 バケットとオブジェクトをプロビジョニングおよび管理して、ROSA ストレージ要件を満たすことができます。OpenShift イメージレジストリオペレーターは、Red Hat OpenShift クラスターの内部レジストリをインストールして管理します。

`ROSAImageRegistryOperatorPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに ROSAImageRegistryOperatorPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 4 月 27 日 20:13 UTC
- 編集日時: 2025 年 5 月 19 日 18:22 UTC
- ARN: arn:aws:iam::aws:policy/service-role/ROSAImageRegistryOperatorPolicy

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ListBuckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSpecificBucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
```

```
        "s3:DeleteBucket",
        "s3:GetBucketTagging",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetBucketLocation",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketTagging",
        "s3:PutEncryptionConfiguration",
        "s3:PutLifecycleConfiguration"
      ],
      "Resource" : [
        "arn:aws:s3:::*-image-registry-${aws:RequestedRegion}-*",
        "arn:aws:s3:::*-image-registry-${aws:RequestedRegion}?",
        "arn:aws:s3:::*-image-registry-${aws:RequestedRegion}"
      ]
    },
    {
      "Sid" : "AllowSpecificObjectActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:ListMultipartUploadParts",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*-image-registry-${aws:RequestedRegion}-*/*",
        "arn:aws:s3:::*-image-registry-${aws:RequestedRegion}?/*",
        "arn:aws:s3:::*-image-registry-${aws:RequestedRegion}/*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

ROSAIngressOperatorPolicy

説明: OpenShift Ingress Operator が Red Hat OpenShift Service on (ROSA) クラスターのロードバランサーとドメインネームシステム AWS (DNS) 設定をプロビジョニングおよび管理できるようにします。このポリシーでは、タグ値への読み取りアクセスを許可します。オペレーターは Route 53 リソースのためにこのタグ値にフィルター処理を行い、ホストゾーンを検出します。

ROSAIngressOperatorPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに ROSAIngressOperatorPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 4 月 20 日 22:37 UTC
- 編集日時: 2025 年 4 月 10 日 23:52 UTC
- ARN: arn:aws:iam::aws:policy/service-role/ROSAIngressOperatorPolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

ROSAInstallerPolicy

説明: Red Hat OpenShift Service on AWS (ROSA) インストーラが ROSA クラスターのインストールをサポートする AWS リソースを管理できるようにします。これには ROSA ワーカーノードのインスタンスプロファイルの管理が含まれます。

`ROSAInstallerPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `ROSAInstallerPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 6 月 6 日 21:00 UTC
- 編集日時: 2025 年 8 月 11 日 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAInstallerPolicy`

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeRegions",
        "ec2:DescribeReservedInstancesOfferings",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeCapacityReservations",
        "elasticloadbalancing:DescribeAccountLimits",
        "elasticloadbalancing:DescribeLoadBalancers",
```

```
        "iam:GetOpenIDConnectProvider",
        "iam:GetRole",
        "route53:GetHostedZone",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName",
        "route53:ListResourceRecordSets",
        "route53:GetAccountLimit",
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassRoleToEC2",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:*:iam::*:role/*-ROSA-Worker-Role"
      ],
      "Effect" : "Allow",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ManageInstanceProfiles",
      "Effect" : "Allow",
      "Action" : [
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:GetInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/rosa-service-managed-*"
      ]
    },
    {
      "Sid" : "CreateInstanceProfiles",
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:CreateInstanceProfile",
        "iam:TagInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/rosa-service-managed-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "GetSecretValue",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "Route53ManageRecords",
      "Effect" : "Allow",
      "Action" : [
        "route53:ChangeResourceRecordSets"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "route53:ChangeResourceRecordSetsNormalizedRecordNames" : [
            "*.openshiftapps.com",
            "*.devshift.org",
            "*.hypershift.local",
            "*.openshiftusgov.com",
            "*.devshiftusgov.com"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "Route53Manage",
      "Effect" : "Allow",
      "Action" : [
        "route53:ChangeTagsForResource",
        "route53:CreateHostedZone",
        "route53:DeleteHostedZone"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances"
          ]
        }
      }
    },
    {
      "Sid" : "RunInstancesNoCondition",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:snapshot/*"
      ]
    },
    {
      "Sid" : "RunInstancesRestrictedRequestTag",
```

```
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "RunInstancesRedHatOwnedAMIs",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:image/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:Owner" : [
            "531415883065",
            "251351625822",
            "210686502322"
          ]
        }
      }
    },
    {
      "Sid" : "ManageInstancesRestrictedResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances",
        "ec2:GetConsoleOutput"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
```

```
    },
    {
      "Sid" : "CreateGrantRestrictedResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com"
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        }
      }
    },
    {
      "Sid" : "ManagedKMSRestrictedResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSecurityGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "DeleteSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "SecurityGroupIngressEgress",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSecurityGroupsVPCNoCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
```

```
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "CreateTagsRestrictedActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateSecurityGroup"
          ]
        }
      }
    },
    {
      "Sid" : "CreateTagsK8sSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "kubernetes.io/cluster/*"
          ]
        }
      }
    },
    {
      "Sid" : "DeleteTagsK8sSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteTags"
      ],
```

```
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "kubernetes.io/cluster/*"
          ]
        }
      }
    },
    {
      "Sid" : "ListPoliciesAttachedToRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

ROSAKMSProviderPolicy

説明: 組み込みの ROSA AWS 暗号化プロバイダーが AWS Key Management Service (KMS) キーを管理して、お客様が用意した KMS AWS キーを使用した etcd データ暗号化をサポートできるようにします。このポリシーでは、KMS キーを使用してデータの暗号化および復号化ができます。

`ROSAKMSProviderPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `ROSAKMSProviderPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 4 月 27 日 20:10 UTC
- 編集日時: 2023 年 4 月 27 日 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAKMSProviderPolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VolumeEncryption",
      "Effect" : "Allow",
      "Action" : [
        "kms:Encrypt",
        "kms:Decrypt",
```

```
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

ROSAKubeControllerPolicy

説明: ROSA Kubernetes コントローラーが ROSA クラスターの Amazon EC2、Elastic Load Balancing (ELB)、および AWS Key Management Service (KMS) リソースを管理できるようにします。

`ROSAKubeControllerPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `ROSAKubeControllerPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 4 月 27 日 20:09 UTC
- 編集日時: 2025 年 4 月 10 日 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAKubeControllerPolicy`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

ROSAManageSubscription

説明: このポリシーは、Red Hat OpenShift Service on AWS (ROSA) サブスクリプションを管理するために必要なアクセス許可を提供します。

ROSAManageSubscription は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに ROSAManageSubscription をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 4 月 11 日 20:58 UTC
- 編集日時: 2023 年 8 月 4 日 19:59 UTC
- ARN: `arn:aws:iam::aws:policy/ROSAManageSubscription`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

ROSANodePoolManagementPolicy

説明: Red Hat OpenShift Service on AWS (ROSA) がクラスター EC2 インスタンスをワーカーノードとして管理できるようにします。これには、セキュリティグループを設定し、インスタンスとボリュームにタグを付けるアクセス許可が含まれます。このポリシーでは、Key Management Service (KMS) AWS キーによって提供されるディスク暗号化で EC2 インスタンスを使用することもできます。

`ROSANodePoolManagementPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `ROSANodePoolManagementPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 6 月 8 日 20:48 UTC
- 編集日時: 2025 年 9 月 9 日 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSANodePoolManagementPolicy`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:*:iam::*:role/aws-service-role/elasticloadbalancing.amazonaws.com/
AWSServiceRoleForElasticLoadBalancing"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
        }
      }
```

```
    },
    {
      "Sid" : "PassWorkerRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:*:iam::*:role/*-ROSA-Worker-Role"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AuthorizeSecurityGroupIngressRestrictedResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:security-group-rule/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "NetworkInterfaces",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "NetworkInterfacesNoCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "TerminateInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances"
          ]
        }
      }
    },
    {
      "Sid" : "CreateTagsCAPAControllerReconcileNetworkInterface",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTagsCAPAControllerReconcileInstance",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTagsCAPAControllerReconcileVolume",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "RunInstancesRequest",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "RunInstancesNoCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:capacity-reservation/*"
      ]
    },
    {
      "Sid" : "RunInstancesRedHatAMI",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:image/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:Owner" : [
            "531415883065",
            "251351625822"
          ]
        }
      }
    },
    {
      "Sid" : "ManagedKMSRestrictedResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/red-hat" : "true"
        }
      }
    },
    {
      "Sid" : "CreateGrantRestricted",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        },
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com"
        }
      }
    }
```

```
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

ROSASharedVPCEndpointPolicy

説明: Red Hat OpenShift Service on AWS (ROSA) インストーラが VPC エンドポイントとセキュリティグループを設定できるようにします。共有 VPC で使用することを目的としています。

`ROSASharedVPCEndpointPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `ROSASharedVPCEndpointPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 8 月 11 日 17:19 UTC
- 編集日時: 2025 年 8 月 11 日 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/ROSASharedVPCEndpointPolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateSecurityGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "DeleteSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
```

```
      }
    },
    {
      "Sid" : "SecurityGroupIngressEgress",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSecurityGroupsVPCNoCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "VPCEndpointWithCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
```

```
    },
    {
      "Sid" : "VPCEndpointResourceTagCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "VPCEndpointNoCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*"
      ]
    },
    {
      "Sid" : "ManageVPCEndpointWithCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint",
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
```

```
    {
      "Sid" : "ModifyVPCEndpoingNoCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Sid" : "CreateTagsRestrictedActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateVpcEndpoint",
            "CreateSecurityGroup"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

ROSASharedVPCRoute53Policy

説明: Red Hat OpenShift Service on AWS (ROSA) インストーラが Route53 レコードを設定できるようにします。共有 VPC で使用することを目的としています。

ROSASharedVPCRoute53Policy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに ROSASharedVPCRoute53Policy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 8 月 11 日 17:19 UTC
- 編集日時: 2025 年 8 月 11 日 17:19 UTC
- ARN: arn:aws:iam::aws:policy/ROSASharedVPCRoute53Policy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
        "route53:ListResourceRecordSets",
        "route53:ListHostedZones",
```

```
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ChangeResourceRecordSetsRestrictedRecordNames",
      "Effect" : "Allow",
      "Action" : [
        "route53:ChangeResourceRecordSets"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "route53:ChangeResourceRecordSetsNormalizedRecordNames" : [
            "*.hypershift.local",
            "*.openshiftapps.com",
            "*.devshift.org",
            "*.openshiftusgov.com",
            "*.devshiftusgov.com"
          ]
        }
      }
    },
    {
      "Sid" : "ChangeTagsForResourceNoCondition",
      "Effect" : "Allow",
      "Action" : [
        "route53:ChangeTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

ROSASRESupportPolicy

説明: ROSA サイト信頼性エンジニアリング (SRE) に、Red Hat OpenShift Service on AWS (ROSA) クラスターに関連する AWS リソースを最初に監視、診断、サポートするために必要なアクセス許可を提供します。これには、ROSA クラスターノードの状態を変更する機能も含まれます。

ROSASRESupportPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに ROSASRESupportPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 6 月 1 日 14:36 UTC
- 編集日時: 2025 年 4 月 10 日 23:52 UTC
- ARN: arn:aws:iam::aws:policy/service-role/ROSASRESupportPolicy

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

ROSAWorkerInstancePolicy

説明: アカウントの Red Hat OpenShift Service on AWS (ROSA) ワーカーノードに Amazon EC2 インスタンスへの読み取り専用アクセスとコンピューティングノードのライフサイクル管理 AWS リージョン を許可します。

`ROSAWorkerInstancePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `ROSAWorkerInstancePolicy` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー

- 作成日時: 2023 年 4 月 20 日 22:35 UTC
- 編集日時: 2025 年 3 月 20 日 23:07 UTC
- ARN: arn:aws:iam::aws:policy/service-role/ROSAWorkerInstancePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2DescribeInstancesRegions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeRegions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ECRGetAuthorizationToken",
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ECRReadOnlyAccessRedHatManaged",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:GetRepositoryPolicy",
```

```
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "ecr:DescribeImages",
        "ecr:BatchGetImage",
        "ecr:ListTagsForResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

Route53RecoveryReadinessServiceRolePolicy

説明: Route 53 リカバリ対応機能のためのサービスリンクロールポリシー

`Route53RecoveryReadinessServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 7 月 15 日 16:06 UTC

- 編集日時: 2023 年 2 月 14 日 18:08 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/Route53RecoveryReadinessServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

Route53ResolverServiceRolePolicy

説明: Route53 Resolver が使用または管理する AWS のサービス およびリソースへのアクセスを有効にします

Route53ResolverServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 8 月 12 日 17:47 UTC
- 編集日時: 2020 年 8 月 12 日 17:47 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/Route53ResolverServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

RTBFabricServiceRolePolicy

説明: AWS RTBFabric がネットワークインターフェイスリソースを作成および管理し、メトリクスを配信するために必要なサービスにリンクされたロール。

RTBFabricServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2025 年 10 月 16 日 16:49 UTC
- 編集日時: 2025 年 10 月 17 日 19:19 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/RTBFabricServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RTBFabricRoleCreateNetworkInterfaceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "RTBFabricRoleCreateTaggedNetworkInterfaceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/RTBFabricManaged" : "true"
        }
      }
    },
    {
      "Sid" : "RTBFabricRoleCreateNetworkInterfacePermissionActions",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterfacePermission",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceTag/RTBFabricManaged" : "true"
        }
      }
    },
    {
      "Sid" : "RTBFabricRoleModifyTaggedNetworkInterfaceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface",
        "ec2:DetachNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/RTBFabricManaged" : "true"
        }
      }
    },
    {
      "Sid" : "RTBFabricRoleTaggingActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        }
      }
    },
    {
      "Sid" : "RTBFabricRoleDescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "RTBFabricRolePutMetricDataActions",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/RTBFabric"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

S3StorageLensServiceRolePolicy

説明: S3 Storage Lens が使用または管理する AWS のサービス およびリソースへのアクセスを有効にします

S3StorageLensServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 11 月 18 日 18:15 UTC
- 編集日時: 2020 年 11 月 18 日 18:15 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/S3StorageLensServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AwsOrgsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

SageMakerStudioAdminIAMConsolePolicy

説明: および SDK を介して Amazon SageMaker Unified Studio の初期管理 AWS マネジメントコンソール 権限と個々のセットアップ権限を提供します。SageMaker Unified Studio Portal の起動を許可します。

SageMakerStudioAdminIAMConsolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに SageMakerStudioAdminIAMConsolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 8 月 18 日 22:49 UTC
- 編集日時: 2025 年 11 月 14 日 22:49 UTC
- ARN: arn:aws:iam::aws:policy/SageMakerStudioAdminIAMConsolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonDataZoneStatement",
      "Effect" : "Allow",
      "Action" : [
        "datazone:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ReadOnlyStatement",
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:ListRoles",
        "iam:GetRole",
        "iam:GetUser"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "IAMPassRoleStatement",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSageMaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:passedToService" : "datazone.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SSMParameterStatement",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:GetParametersByPath",
        "ssm:PutParameter",
        "ssm:DeleteParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/amazon/datazone/q*"
      ]
    },
    {
      "Sid" : "DescribeEc2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeAddresses",
```

```
        "ec2:DescribeNatGateways",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateTaggedEc2Resources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpc"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTaggedSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSubnet"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSubnetInTaggedVPC",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSubnet"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc/*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTaggedSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTaggedSecurityGroupInVPC",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTaggedVPCEndpoint",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "CreateVPCEndpointInTaggedResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "CreateInternetGateway",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateInternetGateway"
      ],
      "Resource" : "arn:aws:ec2:*:*:internet-gateway/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTaggedNatGateway",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNatGateway"
```

```
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:natgateway/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "CreateNatGatewayInTaggedSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNatGateway"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:elastic-ip/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTaggedRouteTable",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateRouteTable"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:route-table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "CreateRouteTableInTaggedSubnet",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateRouteTable"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "AllocateAddress",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress"
      ],
      "Resource" : "arn:aws:ec2:*:*:elastic-ip/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "ModifyTaggedEc2Resources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcAttribute",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "AttachInternetGateway",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachInternetGateway"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:internet-gateway/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "CreateRoute",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateRoute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:route-table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "AssociateRouteTable",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateRouteTable"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
```

```
    },
    {
      "Sid" : "Ec2TaggingOperations",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateVpc",
            "CreateSubnet",
            "CreateSecurityGroup",
            "CreateInternetGateway",
            "CreateNatGateway",
            "CreateRouteTable",
            "CreateVpcEndpoint"
          ],
          "aws:RequestTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "Ec2TagEIP",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:elastic-ip/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "AllowCFNStackCreation",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStacks",
        "cloudformation:ListStackResources",
        "cloudformation:CreateStack",
        "cloudformation:GetTemplateSummary",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "DeleteTaggedVpcResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVpc",
        "ec2:DeleteSubnet",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteInternetGateway",
        "ec2:DetachInternetGateway",
        "ec2:DeleteNatGateway",
        "ec2:DisassociateRouteTable",
        "ec2:DeleteVpcEndpoints",
        "ec2:DeleteRouteTable",
        "ec2:DeleteRoute",
        "ec2:ReleaseAddress"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "DeleteTagsOnTaggedResources",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteTags",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "S3ReadCFNTemplate",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com"
        },
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "KMSReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataZoneKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:datazone:domainId"
        }
      }
    },
    {
      "Sid" : "DataZoneKMSGrantPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
        },
```

```
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:datazone:domainId"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

SageMakerStudioAdminIAMDefaultExecutionPolicy

説明: SageMaker Unified Studio で IAM ロールを使用するための管理実行ポリシー。SageMaker Unified Studio を IAM ベースで使用するために、アカウントのリソースについてプロビジョニング、管理、およびアクセス (データリソースへのアクセスを除く) を管理者に許可します。

`SageMakerStudioAdminIAMDefaultExecutionPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `SageMakerStudioAdminIAMDefaultExecutionPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 8 月 18 日 17:19 UTC
- 編集日時: 2025 年 11 月 18 日 23:34 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioAdminIAMDefaultExecutionPolicy`

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataZone",
      "Effect" : "Allow",
      "Action" : [
        "datazone:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SageMakerUnifiedStudioMcp",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker-unified-studio-mcp:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IamSts",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRoles",
        "iam:GetUser",
        "iam:ListUsers",
        "sts:AssumeRole"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "CreateSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/neptune-graph.amazonaws.com/
AWSServiceRoleForNeptuneGraph",
        "arn:aws:iam::*:role/aws-service-role/redshift.amazonaws.com/
AWSServiceRoleForRedshift",
        "arn:aws:iam::*:role/aws-service-role/sagemaker.amazonaws.com/
AWSServiceRoleForAmazonSageMakerNotebooks",
        "arn:aws:iam::*:role/aws-service-role/ops.emr-serverless.amazonaws.com/
AWSServiceRoleForAmazonEMRServerless",
        "arn:aws:iam::*:role/aws-service-role/airflow.amazonaws.com/
AWSServiceRoleForAmazonMWAA",
        "arn:aws:iam::*:role/aws-service-role/airflow-serverless.amazonaws.com/
AWSServiceRoleForAmazonMWAAServerless",
        "arn:aws:iam::*:role/aws-service-role/elasticmapreduce.amazonaws.com/
AWSServiceRoleForEMRCleanup",
        "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
        "arn:aws:iam::*:role/aws-service-role/observability.aoss.amazonaws.com/
AWSServiceRoleForAmazonOpenSearchServerless",
        "arn:aws:iam::*:role/aws-service-role/ops.athena.amazonaws.com/
AWSServiceRoleForAmazonAthena"
      ]
    },
    {
      "Sid" : "TagRoleAndSession",
      "Effect" : "Allow",
      "Action" : [
        "iam:TagRole",
        "sts:TagSession"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "CreateRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSageMaker*"
      ]
    },
    {
      "Sid" : "AttachPolicy",
      "Effect" : "Allow",
      "Action" : "iam:AttachRolePolicy",
      "Resource" : "arn:aws:iam::*:role/service-role/AmazonSageMaker*",
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/SageMakerStudioUserIAMDefaultExecutionPolicy",
            "arn:aws:iam::aws:policy/SageMakerStudioUserIAMPermissiveExecutionPolicy",
            "arn:aws:iam::aws:policy/service-role/
AmazonS3TablesLakeFormationServiceRole"
          ]
        }
      }
    },
    {
      "Sid" : "SourceIdentity",
      "Effect" : "Allow",
      "Action" : "sts:SetSourceIdentity",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "sts:SourceIdentity" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "PassRoleForProvisioning",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
```

```
            "sagemaker.amazonaws.com",
            "lakeformation.amazonaws.com",
            "athena.amazonaws.com",
            "glue.amazonaws.com",
            "datazone.amazonaws.com",
            "airflow-serverless.amazonaws.com"
          ],
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "PassRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSageMaker*",
        "arn:aws:iam::*:role/${aws:PrincipalTag/AmazonDataZonePassedRolePath}"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "datazone.amazonaws.com",
            "bedrock.amazonaws.com",
            "scheduler.amazonaws.com",
            "emr-serverless.amazonaws.com",
            "redshift.amazonaws.com",
            "airflow-serverless.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "Q",
      "Effect" : "Allow",
      "Action" : [
        "glue:StartCompletion",
        "q:Get*",
        "q:List*",
        "q:PassRequest",
        "q:SendMessage",
        "q:StartConversation"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "SSMParameter",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteParameter",
        "ssm:GetParameter*",
        "ssm:PutParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/amazon/datazone/q*",
        "arn:aws:ssm:*:*:parameter/amazon/datazone/genAI/*",
        "arn:aws:ssm:*::parameter/aws/service/sagemaker-distribution/*"
      ]
    },
    {
      "Sid" : "ManageSageMakerSpace",
      "Effect" : "Allow",
      "Action" : "sagemaker:*",
      "Resource" : [
        "arn:aws:sagemaker:*:*:app/*",
        "arn:aws:sagemaker:*:*:space/*",
        "arn:aws:sagemaker:*:*:domain/*",
        "arn:aws:sagemaker:*:*:user-profile/*"
      ]
    },
    {
      "Sid" : "ResourceGroupsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:GetGroupQuery",
        "resource-groups:ListGroupResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags",
        "sagemaker:Batch*",
        "sagemaker:DeleteTags",
        "sagemaker:Describe*",
        "sagemaker:List*",
```

```
        "sagemaker:Search",
        "sagemaker:*Endpoint*",
        "sagemaker:*Model*",
        "sagemaker:*Context*",
        "sagemaker:*Artifact*",
        "sagemaker:*Action*",
        "sagemaker:*Association*",
        "sagemaker:QueryLineage",
        "sagemaker:*InferenceComponent*",
        "sagemaker:*Job*",
        "sagemaker:StartMlflowTrackingServer",
        "sagemaker:StopMlflowTrackingServer",
        "sagemaker:CreatePresignedMlflowTrackingServerUrl",
        "sagemaker-mlflow:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateBucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucketPolicy",
        "s3:Get*",
        "s3:Put*"
      ],
      "Resource" : [
        "arn:aws:s3:::amazon-sagemaker*"
      ]
    },
    {
      "Sid" : "S3List",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketAcl",
        "s3:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3CrossAccount",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject*",
```

```
        "s3:List*",
        "s3:PutObject*"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CfnManage",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:*"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*"
      ]
    },
    {
      "Sid" : "ValidateCfn",
      "Effect" : "Allow",
      "Action" : "cloudformation:ValidateTemplate",
      "Resource" : "*"
    },
    {
      "Sid" : "LogsAndMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:Describe*",
        "logs:Get*",
        "logs:PutLogEvents",
        "logs:StopQuery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LFManage",
      "Effect" : "Allow",
      "Action" : [
```

```
        "lakeformation:BatchGrantPermissions",
        "lakeformation:BatchRevokePermissions",
        "lakeformation:DeregisterResource",
        "lakeformation:DescribeResource",
        "lakeformation:GetDataAccess",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:GrantPermissions",
        "lakeformation:ListPermissions",
        "lakeformation:ListResources",
        "lakeformation:PutDataLakeSettings",
        "lakeformation:RegisterResource",
        "lakeformation:RevokePermissions",
        "lakeformation:ListLakeFormationOptIns",
        "lakeformation:CreateLakeFormationOptIn",
        "lakeformation:DeleteLakeFormationOptIn"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueDatabase",
      "Effect" : "Allow",
      "Action" : [
        "glue:*"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:connection/*"
      ]
    },
    {
      "Sid" : "GlueLakeFormation",
      "Effect" : "Allow",
      "Action" : [
        "glue:*"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "glue:LakeFormationPermissions" : "Enabled"
        }
      }
```

```
    },
    {
      "Sid" : "Glue",
      "Effect" : "Allow",
      "Action" : [
        "glue:CancelStatement",
        "glue:CreateSession",
        "glue:DeleteSession",
        "glue:Describe*",
        "glue:Get*",
        "glue:List*",
        "glue:NotifyEvent",
        "glue:RunStatement",
        "glue:StartCompletion",
        "glue:StopSession",
        "glue:TagResource",
        "glue:UntagResource",
        "glue:UseGlueStudio",
        "glue:*Job*",
        "glue:TestConnection"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueSessionIsolation",
      "Effect" : "Deny",
      "Action" : [
        "glue:CancelStatement",
        "glue:CreateSession",
        "glue:DeleteSession",
        "glue:GetSession",
        "glue:GetStatement",
        "glue:RunStatement",
        "glue:StopSession",
        "glue:GetDashboardUrl"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:RequestTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}",
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
```

```
      }
    },
    {
      "Sid" : "DenyTaggingUntaggingForeignSessions",
      "Effect" : "Deny",
      "Action" : [
        "glue:TagResource",
        "glue:UntagResource"
      ],
      "Resource" : "arn:aws:glue:*:*:session/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
      }
    },
    {
      "Sid" : "SQLWorkBench",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftData",
      "Effect" : "Allow",
      "Action" : "redshift-data:*",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "redshift-data:statement-owner-iam-userid" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "RedShiftActions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:BatchExecuteStatement",
        "redshift-data:Describe*",
        "redshift-data:ExecuteStatement",
        "redshift-data:List*",
        "redshift-serverless:GetManagedWorkgroup",
```

```
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:List*",
        "redshift:Describe*",
        "redshift:GetClusterCredentialsWithIAM",
        "redshift-serverless:GetCredentials"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Bedrock",
      "Effect" : "Allow",
      "Action" : "bedrock:*",
      "Resource" : "*"
    },
    {
      "Sid" : "FederatedConn",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:List*",
        "dynamodb:Describe*",
        "dynamodb:Scan",
        "dynamodb:PartiQLSelect",
        "dynamodb:Query",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Athena",
      "Effect" : "Allow",
      "Action" : [
        "athena:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AthenaSessionIsolation",
      "Effect" : "Deny",
      "Action" : [
        "athena:StartSession",
        "athena:GetSession",
        "athena:TerminateSession",
        "athena:GetSessionStatus",
```

```
        "athena:GetSessionEndpoint",
        "athena:GetResourceDashboard"
      ],
      "Resource" : [
        "arn:aws:athena:*:*:workgroup/*/session/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:RequestTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}",
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
      }
    },
    {
      "Sid" : "DenyTaggingUntaggingForeignAthenaSessions",
      "Effect" : "Deny",
      "Action" : [
        "athena:TagResource",
        "athena:UntagResource"
      ],
      "Resource" : "arn:aws:athena:*:*:workgroup/*/session/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
      }
    },
    {
      "Sid" : "AirflowServerless",
      "Effect" : "Allow",
      "Action" : [
        "airflow-serverless:List*",
        "airflow-serverless:Get*",
        "airflow-serverless:CreateWorkflow",
        "airflow-serverless:UpdateWorkflow",
        "airflow-serverless:DeleteWorkflow",
        "airflow-serverless:StartWorkflowRun",
        "airflow-serverless:StopWorkflowRun",
        "airflow-serverless:TagResource",
        "airflow-serverless:UntagResource"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "ManagePrivateSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:TagResource",
        "secretsmanager:UpdateSecret",
        "secretsmanager:PutResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "ManageSharedSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:TagResource",
        "secretsmanager:UpdateSecret"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "true"
        }
      }
    },
    {
      "Sid" : "RedshiftSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
```

```
        "secretsmanager:RotateSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:redshift!*"
    },
    {
      "Sid" : "GenerateRecommendations",
      "Effect" : "Allow",
      "Action" : [
        "codewhisperer:GenerateRecommendations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ManageScheduler",
      "Effect" : "Allow",
      "Action" : "scheduler:*",
      "Resource" : "*"
    },
    {
      "Sid" : "Ecr",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:DescribeImages",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeConnectionsAdmin",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:*",
        "codestar-connections:*"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "KmsListAndDescribe",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListGrants"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataZoneKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "kms:Encrypt",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:datazone:domainId"
        }
      }
    },
    {
      "Sid" : "S3Kms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "Null" : {
          "kms:EncryptionContext:aws:s3:arn" : "false"
```

```
        }
      }
    },
    {
      "Sid" : "SchedulerKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:scheduler:schedule:arn" : "false"
        }
      }
    },
    {
      "Sid" : "SecretsKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "secretsmanager.*.amazonaws.com"
        },
        "Null" : {
          "kms:EncryptionContext:SecretARN" : "false"
        }
      }
    },
    {
      "Sid" : "SageMakerKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptTo",
```

```
        "kms:ReEncryptFrom"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "sagemaker.*.amazonaws.com"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "SageMakerCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "sagemaker.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DataZoneCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Encrypt",
            "Decrypt",
            "ReEncryptFrom",
            "ReEncryptTo",
            "GenerateDataKeyWithoutPlaintext",
            "GenerateDataKey",
```

```
            "DescribeKey",
            "RetireGrant",
            "CreateGrant"
          ]
        }
      }
    },
    {
      "Sid" : "GlueKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "glue.*.amazonaws.com"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "BedrockKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
```

```
    {
      "Sid" : "WorkflowsCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:*:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "airflow-serverless.*.amazonaws.com"
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:airflow-serverless:workflow-arn"
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt",
            "Encrypt",
            "GenerateDataKey",
            "GenerateDataKeyWithoutPlaintext",
            "RetireGrant"
          ]
        }
      }
    },
    {
      "Sid" : "WorkflowsKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:*:kms:*:*:key/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:airflow-serverless:workflow-arn"
        }
      }
    },
    {
      "Sid" : "CreateSG",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "SGManage",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "SGAuth",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "Ec2DescribeOnly",
      "Effect" : "Allow",
      "Action" : "ec2:Describe*",
      "Resource" : "*"
    },
    {
      "Sid" : "SGCreateTags",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "aws:cloudformation:*"
          ]
        }
      }
    },
    {
      "Sid" : "VpcAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2TagAccessForVpc",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    },
    {
      "Sid" : "EMRServerless",
      "Effect" : "Allow",
      "Action" : [
        "emr-serverless:ListApplications",
        "emr-serverless:GetApplication"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

SageMakerStudioAdminIAMPermissiveExecutionPolicy

説明: SageMaker Unified Studio で IAM ロールを使用するための管理実行ポリシー。管理者が SageMaker Unified Studio の IAM ベースの使用のために、ローカルアカウントのリソース (S3、Glue、CloudWatch Logs などのデータサービス内のすべての API への広範なアクセスを含む) についてプロビジョニング、管理、およびアクセスできるようにします。

`SageMakerStudioAdminIAMPermissiveExecutionPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `SageMakerStudioAdminIAMPermissiveExecutionPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 8 月 18 日 17:19 UTC
- 編集日時: 2025 年 11 月 18 日 23:34 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioAdminIAMPermissiveExecutionPolicy`

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:*",
        "glue:*",
        "logs:*",
        "redshift-data:*",
        "redshift-serverless:*",
        "redshift:*",
        "s3:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ComputeAccess",
      "Effect" : "Allow",
      "Action" : [
        "athena:*",
        "bedrock:*",
        "codewhisperer:*",
        "sagemaker-unified-studio-mcp:*",
        "datazone:*",
        "q:*",
        "sagemaker:*",
        "sagemaker-mlflow:*",
        "scheduler:*",
        "sqlworkbench:*",
        "emr-serverless:*",
        "airflow-serverless:*"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "CfnManage",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:*"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*"
      ]
    },
    {
      "Sid" : "ValidateCfn",
      "Effect" : "Allow",
      "Action" : "cloudformation:ValidateTemplate",
      "Resource" : "*"
    },
    {
      "Sid" : "GlueSessionIsolation",
      "Effect" : "Deny",
      "Action" : [
        "glue:CancelStatement",
        "glue:CreateSession",
        "glue:DeleteSession",
        "glue:GetSession",
        "glue:GetStatement",
        "glue:RunStatement",
        "glue:StopSession",
        "glue:GetDashboardUrl"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:RequestTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}",
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
      }
    },
    {
      "Sid" : "DenyTaggingUntaggingForeignSessions",
      "Effect" : "Deny",
      "Action" : [
        "glue:TagResource",
        "glue:UntagResource"
```

```
      ],
      "Resource" : "arn:aws:glue:*:*:session/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
      }
    },
    {
      "Sid" : "IamSts",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRoles",
        "iam:GetUser",
        "iam:ListUsers",
        "sts:AssumeRole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/neptune-graph.amazonaws.com/
AWSServiceRoleForNeptuneGraph",
        "arn:aws:iam::*:role/aws-service-role/redshift.amazonaws.com/
AWSServiceRoleForRedshift",
        "arn:aws:iam::*:role/aws-service-role/sagemaker.amazonaws.com/
AWSServiceRoleForAmazonSageMakerNotebooks",
        "arn:aws:iam::*:role/aws-service-role/ops.emr-serverless.amazonaws.com/
AWSServiceRoleForAmazonEMRServerless",
        "arn:aws:iam::*:role/aws-service-role/airflow.amazonaws.com/
AWSServiceRoleForAmazonMWAA",
        "arn:aws:iam::*:role/aws-service-role/airflow-serverless.amazonaws.com/
AWSServiceRoleForAmazonMWAAServerless",
        "arn:aws:iam::*:role/aws-service-role/elasticmapreduce.amazonaws.com/
AWSServiceRoleForEMRCleanup",
        "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
        "arn:aws:iam::*:role/aws-service-role/observability.aoss.amazonaws.com/
AWSServiceRoleForAmazonOpenSearchServerless",
```

```
        "arn:aws:iam::*:role/aws-service-role/ops.athena.amazonaws.com/
AWSServiceRoleForAmazonAthena"
      ]
    },
    {
      "Sid" : "TagRoleAndSession",
      "Effect" : "Allow",
      "Action" : [
        "iam:TagRole",
        "sts:TagSession"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        }
      }
    },
    {
      "Sid" : "PassRoleForProvisioning",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com",
            "lakeformation.amazonaws.com",
            "athena.amazonaws.com",
            "glue.amazonaws.com",
            "datazone.amazonaws.com",
            "airflow-serverless.amazonaws.com"
          ],
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "PassRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
```

```
        "arn:aws:iam::*:role/service-role/AmazonSageMaker*",
        "arn:aws:iam::*:role/${aws:PrincipalTag/AmazonDataZonePassedRolePath}"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "bedrock.amazonaws.com",
            "datazone.amazonaws.com",
            "redshift-serverless.amazonaws.com",
            "redshift.amazonaws.com",
            "scheduler.amazonaws.com",
            "emr-serverless.amazonaws.com",
            "airflow-serverless.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreateRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSageMaker*"
      ]
    },
    {
      "Sid" : "AttachPolicy",
      "Effect" : "Allow",
      "Action" : "iam:AttachRolePolicy",
      "Resource" : "arn:aws:iam::*:role/service-role/AmazonSageMaker*",
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/SageMakerStudioUserIAMDefaultExecutionPolicy",
            "arn:aws:iam::aws:policy/SageMakerStudioUserIAMPermissiveExecutionPolicy",
            "arn:aws:iam::aws:policy/service-role/
AmazonS3TablesLakeFormationServiceRole"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "SourceIdentity",
      "Effect" : "Allow",
      "Action" : "sts:SetSourceIdentity",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "sts:SourceIdentity" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "SSM",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteParameter",
        "ssm:GetParameter*",
        "ssm:PutParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/amazon/datazone/q*",
        "arn:aws:ssm:*:*:parameter/amazon/datazone/genAI/*",
        "arn:aws:ssm:*::parameter/aws/service/sagemaker-distribution/*"
      ]
    },
    {
      "Sid" : "LFAccess",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:BatchGrantPermissions",
        "lakeformation:BatchRevokePermissions",
        "lakeformation:DeregisterResource",
        "lakeformation:DescribeResource",
        "lakeformation:GetDataAccess",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:GrantPermissions",
        "lakeformation:ListPermissions",
        "lakeformation:ListResources",
        "lakeformation:PutDataLakeSettings",
        "lakeformation:RegisterResource",
        "lakeformation:RevokePermissions",
        "lakeformation:ListLakeFormationOptIns",
        "lakeformation:CreateLakeFormationOptIn",
        "lakeformation:DeleteLakeFormationOptIn"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "FederatedConn",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:List*",
        "dynamodb:Describe*",
        "dynamodb:Scan",
        "dynamodb:PartiQLSelect",
        "dynamodb:Query",
        "secretsmanager:ListSecrets",
        "resource-groups:GetGroupQuery",
        "resource-groups:ListGroupResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ManagePrivateSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:TagResource",
        "secretsmanager:UpdateSecret",
        "secretsmanager:PutResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "ManageSharedSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
```

```
        "secretsmanager:TagResource",
        "secretsmanager:UpdateSecret"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "true"
        }
      }
    },
    {
      "Sid" : "RedshiftSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:RotateSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:redshift!*"
    },
    {
      "Sid" : "Ecr",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:DescribeImages",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeConnections",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:*",
        "codestar-connections:*"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KmsListAndDescribe",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListGrants"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataZoneKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "kms:Encrypt",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:datazone:domainId"
        }
      }
    },
    {
      "Sid" : "S3Kms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
```

```
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "Null" : {
          "kms:EncryptionContext:aws:s3:arn" : "false"
        }
      }
    },
    {
      "Sid" : "SchedulerKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:scheduler:schedule:arn" : "false"
        }
      }
    },
    {
      "Sid" : "SecretsKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "secretsmanager.*.amazonaws.com"
        },
        "Null" : {
          "kms:EncryptionContext:SecretARN" : "false"
        }
      }
    },
    {
      "Sid" : "SageMakerKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
```

```
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "sagemaker.*.amazonaws.com"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "SageMakerCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "sagemaker.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DataZoneCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Encrypt",
            "Decrypt",
```

```
            "ReEncryptFrom",
            "ReEncryptTo",
            "GenerateDataKeyWithoutPlaintext",
            "GenerateDataKey",
            "DescribeKey",
            "RetireGrant",
            "CreateGrant"
          ]
        }
      }
    },
    {
      "Sid" : "GlueKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "glue.*.amazonaws.com"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "BedrockKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com"
        },
        "Null" : {
```

```
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "WorkflowsCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:*:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "airflow-serverless.*.amazonaws.com"
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:airflow-serverless:workflow-arn"
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt",
            "Encrypt",
            "GenerateDataKey",
            "GenerateDataKeyWithoutPlaintext",
            "RetireGrant"
          ]
        }
      }
    },
    {
      "Sid" : "WorkflowsKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:*:kms:*:*:key/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:airflow-serverless:workflow-arn"
        }
      }
```

```
    },
    {
      "Sid" : "CreateSG",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "SGManage",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "SGAuth",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "Ec2DescribeOnly",
      "Effect" : "Allow",
      "Action" : "ec2:Describe*",
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "SGCreateTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "aws:cloudformation:*"
          ]
        }
      }
    },
    {
      "Sid" : "VpcAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2TagAccessForVpc",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    },
    {
      "Sid" : "AthenaSessionIsolation",
      "Effect" : "Deny",
      "Action" : [
```

```
        "athena:StartSession",
        "athena:GetSession",
        "athena:TerminateSession",
        "athena:GetSessionStatus",
        "athena:GetSessionEndpoint",
        "athena:GetResourceDashboard"
      ],
      "Resource" : [
        "arn:aws:athena:*:*:workgroup/*/session/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:RequestTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}",
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
      }
    },
    {
      "Sid" : "DenyTaggingUntaggingForeignAthenaSessions",
      "Effect" : "Deny",
      "Action" : [
        "athena:TagResource",
        "athena:UntagResource"
      ],
      "Resource" : "arn:aws:athena:*:*:workgroup/*/session/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

SageMakerStudioAdminProjectUserRolePolicy

説明: この IAM ポリシーは、データレイクオペレーションの AWS Glue データカタログ (メタデータ) と Amazon S3 (実際のデータ) へのフルアクセスを IAM ロールに付与します。アクセスの範囲はアカウント、ロールタグです。

SageMakerStudioAdminProjectUserRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに SageMakerStudioAdminProjectUserRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 7 月 9 日 20:52 UTC
- 編集日時: 2025 年 7 月 10 日 23:52 UTC
- ARN: arn:aws:iam::aws:policy/SageMakerStudioAdminProjectUserRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GlueDatalakePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateTable",
        "glue:DeleteTable",
        "glue:BatchDeleteTable",
```

```
        "glue:UpdateTable",
        "glue:BatchCreatePartition",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
        "glue:UpdatePartition",
        "glue:BatchGetPartition",
        "glue:BatchGetTableOptimizer",
        "glue:GetCatalogImportStatus",
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:GetColumnStatisticsTaskRun",
        "glue:GetColumnStatisticsTaskRuns",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetPartition",
        "glue:GetPartitionIndexes",
        "glue:GetPartitions",
        "glue:GetTable",
        "glue:GetTableOptimizer",
        "glue:GetTableVersion",
        "glue:GetTableVersions",
        "glue:GetTables",
        "glue:SearchTables",
        "glue:ListTableOptimizerRuns",
        "glue:CreatePartitionIndex",
        "glue:BatchUpdatePartition",
        "glue:DeleteTableVersion",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeletePartitionIndex",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:BatchDeleteTableVersion",
        "glue:GetCatalogs",
        "glue:GetCatalog"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "aws:PrincipalTag/BootstrappedServices" : "*glue*"
        }
      }
    },
    {
      "Sid" : "GlueCatalogDatabasePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:DeleteDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "aws:PrincipalTag/BootstrappedServices" : "*glue*"
        }
      }
    },
    {
      "Sid" : "DataAccessPermissionsForS3",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject",
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "aws:PrincipalTag/BootstrappedServices" : "*glue*"
        }
```

```
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

SageMakerStudioBedrockAgentServiceRolePolicy

説明: Amazon Bedrock エージェントが SageMaker Studio のエージェントにアタッチされた Amazon Bedrock モデルやその他のリソースにアクセスできるようにします。

`SageMakerStudioBedrockAgentServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `SageMakerStudioBedrockAgentServiceRolePolicy` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2025 年 2 月 13 日 23:37 UTC
- 編集日時: 2025 年 2 月 13 日 23:37 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockAgentServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockAppInferenceProfileInvocationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetInferenceProfile",
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : "arn:aws:bedrock:*:*:application-inference-profile/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockModelInvocationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*",
        "arn:aws:bedrock:*:*:custom-model/*",
        "arn:aws:bedrock:*:*:provisioned-model/*"
      ],
      "Condition" : {
        "Null" : {
          "bedrock:InferenceProfileArn" : "false"
        }
      }
    },
```

```
    {
      "Sid" : "BedrockApplyGuardrailPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:ApplyGuardrail",
      "Resource" : "arn:aws:bedrock:*:*:guardrail/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockRetrieveAndGeneratePermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:RetrieveAndGenerate",
      "Resource" : "*"
    },
    {
      "Sid" : "LambdaInvokeFunctionInProjectPermissions",
      "Effect" : "Allow",
      "Action" : "lambda:InvokeFunction",
      "Resource" : "arn:aws:lambda:*:*:function:amazon-bedrock*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockRetrievePermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:Retrieve",
      "Resource" : "arn:aws:bedrock:*:*:knowledge-base/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
```

```
    },
    {
      "Sid" : "S3GetObjectPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionAttributes",
        "s3:GetObjectAttributes"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        }
      }
    },
    {
      "Sid" : "BedrockGuardrailKmsPermissions",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContext:aws:bedrock:guardrail-id" : "false"
        }
      }
    },
    {
      "Sid" : "S3KmsPermissions",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
```

```
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : [
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/*"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

SageMakerStudioBedrockChatAgentUserRolePolicy

説明: SageMaker Studio 内での Amazon Bedrock チャットエージェントアプリの設定と Amazon Bedrock エージェントへのアクセスを提供します。

SageMakerStudioBedrockChatAgentUserRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに SageMakerStudioBedrockChatAgentUserRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2025 年 2 月 13 日 23:52 UTC

- 編集日時: 2025 年 2 月 13 日 23:52 UTC
- ARN: arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockChatAgentUserRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockGetAgentAliasPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:GetAgentAlias",
      "Resource" : "arn:aws:bedrock:*:*:agent-alias/${aws:PrincipalTag/AgentId}/
${aws:PrincipalTag/AgentAliasId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockInvokeAgentPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:InvokeAgent",
      "Resource" : "arn:aws:bedrock:*:*:agent-alias/${aws:PrincipalTag/AgentId}/
${aws:PrincipalTag/AgentAliasId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
```

```
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockGetAndListAgentMetadataPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetAgent",
        "bedrock:GetAgentActionGroup",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:GetAgentVersion",
        "bedrock:ListAgentActionGroups",
        "bedrock:ListAgentAliases",
        "bedrock:ListAgentKnowledgeBases",
        "bedrock:ListAgentVersions"
      ],
      "Resource" : "arn:aws:bedrock:*:*:agent/${aws:PrincipalTag/AgentId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "S3ListAppDefinitionPermissions",
      "Effect" : "Allow",
      "Action" : "s3:ListBucket",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringEquals" : {
          "s3:prefix" : "${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/
AmazonDataZoneProject}/${aws:PrincipalTag/AppDefinitionPath}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : "",
          "aws:PrincipalTag/AppDefinitionPath" : ""
        }
```

```
      }
    },
    {
      "Sid" : "S3GetAppDefinitionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/
${aws:PrincipalTag/AppDefinitionPath}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : "",
          "aws:PrincipalTag/AppDefinitionPath" : ""
        }
      }
    },
    {
      "Sid" : "S3ListDataSourcePermissions",
      "Effect" : "Allow",
      "Action" : "s3:ListBucket",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringEquals" : {
          "s3:prefix" : "${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/
AmazonDataZoneProject}/${aws:PrincipalTag/DataSourcePath}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : "",
          "aws:PrincipalTag/DataSourcePath" : ""
        }
      }
    },
    {
```

```
      "Sid" : "S3GetDataSourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/
${aws:PrincipalTag/DataSourcePath}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : "",
          "aws:PrincipalTag/DataSourcePath" : ""
        }
      }
    },
    {
      "Sid" : "BedrockAgentKmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com",
          "kms:EncryptionContext:aws:bedrock:arn" : "arn:aws:bedrock:*:
${aws:PrincipalAccount}:agent/${aws:PrincipalTag/AgentId}"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3KmsPermissions",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
```

```
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : [
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/*"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

SageMakerStudioBedrockEvaluationJobServiceRolePolicy

説明: Amazon Bedrock が SageMaker Studio 内の評価ジョブの Amazon Bedrock モデルとデータセットにアクセスできるようにします。

`SageMakerStudioBedrockEvaluationJobServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `SageMakerStudioBedrockEvaluationJobServiceRolePolicy` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2025 年 2 月 14 日 00:37 UTC
- 編集日時: 2025 年 2 月 14 日 00:37 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockEvaluationJobServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockEvaluationInferenceProfileInvocationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream",
        "bedrock:GetInferenceProfile"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:application-inference-profile/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
```

```
      "Sid" : "BedrockInvokeModelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*",
        "arn:aws:bedrock:*:*:custom-model/*",
        "arn:aws:bedrock:*:*:provisioned-model/*"
      ],
      "Condition" : {
        "Null" : {
          "bedrock:InferenceProfileArn" : "false"
        }
      }
    },
    {
      "Sid" : "BedrockModelInvocationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateModelInvocationJob",
        "bedrock:StopModelInvocationJob",
        "bedrock:GetProvisionedModelThroughput"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3GetBucketLocationPermissions",
      "Effect" : "Allow",
      "Action" : "s3:GetBucketLocation",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : ""
        }
```

```
      }
    },
    {
      "Sid" : "S3ListBucketPermissions",
      "Effect" : "Allow",
      "Action" : "s3:ListBucket",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "s3:prefix" : "${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/
AmazonDataZoneProject}/*"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        }
      }
    },
    {
      "Sid" : "S3EvaluationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:ListMultipartUploadParts",
        "s3:AbortMultipartUpload"
      ],
      "Resource" : [
        "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/${aws:PrincipalTag/
AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        }
```

```
      }
    },
    {
      "Sid" : "KmsDescribeKeyPermissions",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3KmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : [
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/*"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

SageMakerStudioBedrockFlowServiceRolePolicy

説明: Amazon Bedrock Flows が SageMaker Studio 内のフローにアタッチされた Amazon Bedrock モデルやその他のリソースにアクセスできるようにします。

SageMakerStudioBedrockFlowServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに SageMakerStudioBedrockFlowServiceRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2025 年 2 月 14 日 00:07 UTC
- 編集日時: 2025 年 4 月 9 日 20:37 UTC
- ARN: arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockFlowServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockPromptPermissions",
```

```
      "Effect" : "Allow",
      "Action" : "bedrock:GetPrompt",
      "Resource" : "arn:aws:bedrock:*:*:prompt/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockKnowledgeBasePermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:Retrieve",
      "Resource" : "arn:aws:bedrock:*:*:knowledge-base/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockGuardrailPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:ApplyGuardrail",
      "Resource" : "arn:aws:bedrock:*:*:guardrail/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "AllowBedrockRetrieveAndGeneratePermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:RetrieveAndGenerate",
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "AllowLambdaInvokeFunctionInProjectPermissions",
      "Effect" : "Allow",
      "Action" : "lambda:InvokeFunction",
      "Resource" : "arn:aws:lambda:*:*:function:amazon-bedrock*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "AllowBedrockApplicationInferenceProfileAccessInProjectPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetInferenceProfile",
        "bedrock:InvokeModel"
      ],
      "Resource" : "arn:aws:bedrock:*:*:application-inference-profile/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "AllowBedrockInvokeModelAccessWithInferenceProfilePermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:InvokeModel",
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*",
        "arn:aws:bedrock:*:*:custom-model/*",
        "arn:aws:bedrock:*:*:provisioned-model/*"
      ],
      "Condition" : {
        "Null" : {
          "bedrock:InferenceProfileArn" : "false"
        }
      }
    },
    {
      "Sid" : "BedrockInvokeAgentPermissions",
```

```
      "Effect" : "Allow",
      "Action" : "bedrock:InvokeAgent",
      "Resource" : "arn:aws:bedrock:*:*:agent-alias/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockPromptKmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com",
          "kms:EncryptionContext:aws:bedrock-prompts:arn" : "arn:aws:bedrock:*:
${aws:PrincipalAccount}:prompt/*"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BedrockGuardrailKmsPermissions",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContext:aws:bedrock:guardrail-id" : "false"
```

```
        }
      }
    },
    {
      "Sid" : "BedrockAgentKmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com",
          "kms:EncryptionContext:aws:bedrock:arn" : "arn:aws:bedrock:*:
${aws:PrincipalAccount}:agent/*"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

SageMakerStudioBedrockFunctionExecutionRolePolicy

説明: AWS Lambda が SageMaker Studio で Amazon Bedrock 関数コンポーネントの設定にアクセスできるようにします。

SageMakerStudioBedrockFunctionExecutionRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに SageMakerStudioBedrockFunctionExecutionRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2025 年 2 月 25 日 03:52 UTC
- 編集日時: 2025 年 2 月 25 日 03:52 UTC
- ARN: arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockFunctionExecutionRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecretsManagerReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:amazon-bedrock*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
```

```
      }
    },
    {
      "Sid" : "KMSSameAccountBedrockViaSecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "secretsmanager.*.amazonaws.com",
          "kms:EncryptionContext:SecretARN" : "arn:aws:secretsmanager:*:
${aws:PrincipalAccount}:secret:amazon-bedrock*"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

SageMakerStudioBedrockKnowledgeBaseCustomResourcePolicy

説明: SageMaker Studio でベクトルストアと Amazon Bedrock ナレッジベースを設定するアクセスを提供します。

SageMakerStudioBedrockKnowledgeBaseCustomResourcePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに SageMakerStudioBedrockKnowledgeBaseCustomResourcePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2025 年 2 月 25 日 03:37 UTC
- 編集日時: 2025 年 2 月 25 日 03:37 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockKnowledgeBaseCustomResourcePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "OpenSearchServerlessPermissions",
      "Effect" : "Allow",
      "Action" : "aoss:APIAccessAll",
      "Resource" : "arn:aws:aoss:*:*:collection/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "aoss:collection" : "bedrock*"
        }
      }
    },
    {
      "Sid" : "BedrockKnowledgeBasePermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetIngestionJob",
```

```
        "bedrock:ListIngestionJobs",
        "bedrock:StartIngestionJob"
      ],
      "Resource" : "arn:aws:bedrock:*:*:knowledge-base/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy

説明: Amazon Bedrock ナレッジベースが SageMaker Studio の Amazon Bedrock モデルとデータソースにアクセスできるようにします。

`SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2025 年 2 月 25 日 02:52 UTC

- 編集日時: 2025 年 7 月 15 日 17:22 UTC
- ARN: arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockAppInferenceProfileInvocationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetInferenceProfile",
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : "arn:aws:bedrock:*:*:application-inference-profile/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockModelInvocationPermission",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : [
```

```
        "arn:aws:bedrock:*::foundation-model/*",
        "arn:aws:bedrock:*:*:custom-model/*",
        "arn:aws:bedrock:*:*:provisioned-model/*"
      ],
      "Condition" : {
        "Null" : {
          "bedrock:InferenceProfileArn" : "false"
        }
      }
    },
    {
      "Sid" : "OpenSearchServerlessPermissions",
      "Effect" : "Allow",
      "Action" : "aoss:APIAccessAll",
      "Resource" : "arn:aws:aoss:*:*:collection/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "aoss:collection" : "bedrock*"
        }
      }
    },
    {
      "Sid" : "ListDomainS3BucketPermissions",
      "Effect" : "Allow",
      "Action" : "s3:ListBucket",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "s3:prefix" : [
            "${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/
AmazonDataZoneProject}",
            "${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/
AmazonDataZoneProject}/*"
          ]
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
```

```
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        }
      }
    },
    {
      "Sid" : "AccessDomainS3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        }
      }
    },
    {
      "Sid" : "VectorStoresKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "neptune-graph.*.amazonaws.com",
            "s3vectors.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
```

```
        }
      }
    },
    {
      "Sid" : "VectorStoresKmsDescribeKey",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "neptune-graph.*.amazonaws.com",
            "s3vectors.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "NeptuneGraphDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "neptune-graph:GetGraph",
        "neptune-graph:DeleteDataViaQuery",
        "neptune-graph:WriteDataViaQuery",
        "neptune-graph:ReadDataViaQuery"
      ],
      "Resource" : "arn:aws:neptune-graph:*:*:graph/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "S3VectorsDataAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3vectors:GetVectorBucket",
        "s3vectors:GetIndex",
        "s3vectors:PutVectors",
        "s3vectors:GetVectors",
        "s3vectors:ListVectors",
        "s3vectors:QueryVectors",
        "s3vectors:DeleteVectors"
      ],
      "Resource" : "arn:aws:s3vectors:*:*:bucket/amazon-bedrock-ide-${aws:PrincipalTag/
AmazonDataZoneProject}*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BedrockKnowledgeBaseKmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:EncryptionContext:aws:bedrock:arn" : "arn:aws:bedrock:*:
${aws:PrincipalAccount}:knowledge-base/*"
        }
      }
    },
    {
      "Sid" : "S3KmsPermissions",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
```

```
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : [
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/*"
          ]
        }
      }
    },
    {
      "Sid" : "SqlWorkbenchAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:GetSqlRecommendations",
        "sqlworkbench:PutSqlGenerationContext",
        "sqlworkbench:GetSqlGenerationContext",
        "sqlworkbench:DeleteSqlGenerationContext"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BedrockGenerateQueryPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GenerateQuery"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

SageMakerStudioBedrockPromptUserRolePolicy

説明: SageMaker Studio の Amazon Bedrock プロンプトとその設定へのアクセスを提供します。

SageMakerStudioBedrockPromptUserRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに SageMakerStudioBedrockPromptUserRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2025 年 2 月 14 日 00:22 UTC
- 編集日時: 2025 年 2 月 14 日 00:22 UTC
- ARN: arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockPromptUserRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockPromptReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:GetPrompt",
      "Resource" : "arn:aws:bedrock:*:*:prompt/${aws:PrincipalTag/PromptId}:
${aws:PrincipalTag/PromptVersion}",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "S3ListPromptDefinitionPermissions",
      "Effect" : "Allow",
      "Action" : "s3:ListBucket",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringEquals" : {
          "s3:prefix" : "${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/
AmazonDataZoneProject}/${aws:PrincipalTag/PromptDefinitionPath}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : "",
          "aws:PrincipalTag/PromptDefinitionPath" : ""
        }
      }
    },
    {
      "Sid" : "S3GetPromptDefinitionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/
${aws:PrincipalTag/PromptDefinitionPath}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : "",
          "aws:PrincipalTag/PromptDefinitionPath" : ""
```

```
        }
      }
    },
    {
      "Sid" : "BedrockPromptKmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com",
          "kms:EncryptionContext:aws:bedrock-prompts:arn" : "arn:aws:bedrock:*:
${aws:PrincipalAccount}:prompt/${aws:PrincipalTag/PromptId}"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3KmsPermissions",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : [
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/*"
          ]
        }
      }
    }
  ]
```

```
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

SageMakerStudioDomainExecutionRolePolicy

説明: このポリシーは、Amazon SageMaker Studio による Amazon SageMaker ドメイン内のデータのカタログ化、検出、管理、共有、分析に使用されます。

`SageMakerStudioDomainExecutionRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `SageMakerStudioDomainExecutionRolePolicy` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2024 年 11 月 20 日 21:56 UTC
- 編集日時: 2025 年 11 月 18 日 21:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioDomainExecutionRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataZonePermissions",
      "Effect" : "Allow",
      "Action" : [
        "datazone:AcceptPredictions",
        "datazone:AcceptSubscriptionRequest",
        "datazone:AddEntityOwner",
        "datazone:AddPolicyGrant",
        "datazone:AssociateGovernedTerms",
        "datazone:BatchGetAttributesMetadata",
        "datazone:BatchPutAttributesMetadata",
        "datazone:CancelMetadataGenerationRun",
        "datazone:CancelSubscription",
        "datazone:CreateAsset",
        "datazone:CreateAssetFilter",
        "datazone:CreateAssetRevision",
        "datazone:CreateAssetType",
        "datazone:CreateConnection",
        "datazone:CreateDataProduct",
        "datazone:CreateDataProductRevision",
        "datazone:CreateDataSource",
        "datazone:CreateDomainUnit",
        "datazone:CreateEnvironment",
        "datazone:CreateEnvironmentProfile",
        "datazone:CreateFormType",
        "datazone:CreateGlossary",
        "datazone:CreateGlossaryTerm",
        "datazone:CreateListingChangeSet",
        "datazone:CreateProject",
        "datazone:CreateProjectMembership",
        "datazone:CreateRule",
        "datazone:CreateSubscriptionGrant",
        "datazone:CreateSubscriptionRequest",
        "datazone:DeleteAsset",
        "datazone:DeleteAssetFilter",
        "datazone:DeleteAssetType",
        "datazone:DeleteConnection",
        "datazone:DeleteDataProduct",
```

```
            "datazone:DeleteDataSource",
            "datazone:DeleteDomainUnit",
            "datazone:DeleteEnvironment",
            "datazone:DeleteEnvironmentProfile",
            "datazone:DeleteFormType",
            "datazone:DeleteGlossary",
            "datazone:DeleteGlossaryTerm",
            "datazone:DeleteListing",
            "datazone:DeleteProject",
            "datazone:DeleteProjectMembership",
            "datazone:DeleteRule",
            "datazone:DeleteSubscriptionGrant",
            "datazone:DeleteSubscriptionRequest",
            "datazone:DeleteSubscriptionTarget",
            "datazone:DeleteTimeSeriesDataPoints",
            "datazone:DisassociateGovernedTerms",
            "datazone:GetAsset",
            "datazone:GetAssetFilter",
            "datazone:GetAssetType",
            "datazone:GetConnection",
            "datazone:GetDataProduct",
            "datazone:GetDataSource",
            "datazone:GetDataSourceRun",
            "datazone:GetDomain",
            "datazone:GetDomainUnit",
            "datazone:GetEnvironment",
            "datazone:GetEnvironmentAction",
            "datazone:GetEnvironmentActionLink",
            "datazone:GetEnvironmentBlueprint",
            "datazone:GetEnvironmentBlueprintConfiguration",
            "datazone:GetEnvironmentCredentials",
            "datazone:GetEnvironmentProfile",
            "datazone:GetFormType",
            "datazone:GetGlossary",
            "datazone:GetGlossaryTerm",
            "datazone:GetGroupProfile",
            "datazone:GetLineageNode",
            "datazone:GetListing",
            "datazone:GetMetadataGenerationRun",
            "datazone:GetProject",
            "datazone:GetRule",
            "datazone:GetSubscription",
            "datazone:GetSubscriptionEligibility",
            "datazone:GetSubscriptionGrant",
```

```
        "datazone:GetSubscriptionRequestDetails",
        "datazone:GetSubscriptionTarget",
        "datazone:GetTimeSeriesDataPoint",
        "datazone:GetUpdateEligibility",
        "datazone:GetUserProfile",
        "datazone:ListAccountEnvironments",
        "datazone:ListAssetFilters",
        "datazone:ListAssetRevisions",
        "datazone:ListConnections",
        "datazone:ListDataProductRevisions",
        "datazone:ListDataSourceRunActivities",
        "datazone:ListDataSourceRuns",
        "datazone:ListDataSources",
        "datazone:ListDomainUnitsForParent",
        "datazone:ListEntityOwners",
        "datazone:ListEnvironmentActions",
        "datazone:ListEnvironmentBlueprintConfigurationSummaries",
        "datazone:ListEnvironmentBlueprintConfigurations",
        "datazone:ListEnvironmentBlueprints",
        "datazone:ListEnvironmentProfiles",
        "datazone:ListEnvironments",
        "datazone:ListGroupsForUser",
        "datazone:ListLineageNodeHistory",
        "datazone:ListMetadataGenerationRuns",
        "datazone:ListNotifications",
        "datazone:ListPolicyGrants",
        "datazone:ListProjectMemberships",
        "datazone:ListProjects",
        "datazone:ListRules",
        "datazone:ListSubscriptionGrants",
        "datazone:ListSubscriptionRequests",
        "datazone:ListSubscriptionTargets",
        "datazone:ListSubscriptions",
        "datazone:ListTimeSeriesDataPoints",
        "datazone:ListWarehouseMetadata",
        "datazone:RejectPredictions",
        "datazone:RejectSubscriptionRequest",
        "datazone:RemoveEntityOwner",
        "datazone:RemovePolicyGrant",
        "datazone:RevokeSubscription",
        "datazone:Search",
        "datazone:SearchGroupProfiles",
        "datazone:SearchListings",
        "datazone:SearchRules",
```

```
        "datazone:SearchTypes",
        "datazone:SearchUserProfiles",
        "datazone:StartDataSourceRun",
        "datazone:StartMetadataGenerationRun",
        "datazone:UpdateAssetFilter",
        "datazone:UpdateConnection",
        "datazone:UpdateDataSource",
        "datazone:UpdateDomainUnit",
        "datazone:UpdateEnvironment",
        "datazone:UpdateEnvironmentDeploymentStatus",
        "datazone:UpdateEnvironmentProfile",
        "datazone:UpdateGlossary",
        "datazone:UpdateGlossaryTerm",
        "datazone:UpdateProject",
        "datazone:UpdateRule",
        "datazone:UpdateSubscriptionGrantStatus",
        "datazone:UpdateSubscriptionRequest"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RAMResourceShareStatement",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShareAssociations",
        "ram:GetResourceShares"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonQPermissionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "q:StartConversation",
        "q:SendMessage",
        "q:ListConversations",
        "q:GetConversation",
        "q:PassRequest",
        "q:GetIdentityMetadata",
        "glue:StartCompletion",
        "glue:GetCompletion"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "AllowSetTrustedIdentity",
      "Effect" : "Allow",
      "Action" : [
        "sts:SetContext"
      ],
      "Resource" : "arn:aws:sts::*:self"
    },
    {
      "Sid" : "SSMGetParameterStatement",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/amazon/datazone/q/${aws:PrincipalTag/datazone-
domainId}*",
        "arn:aws:ssm:*:*:parameter/amazon/datazone/genAI/${aws:PrincipalTag/datazone-
domainId}/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GetCodeConnectionsPermissionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:GetConnection",
        "codeconnections:GetHost",
        "codestar-connections:GetConnection",
        "codestar-connections:GetHost"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "false"
        },
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
```

```
    },
    {
      "Sid" : "ListCodeConnectionsPermissionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:ListConnections",
        "codeconnections:ListTagsForResource",
        "codestar-connections:ListConnections",
        "codestar-connections:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "UseCodeConnectionsPermissionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:UseConnection",
        "codestar-connections:UseConnection"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "false"
        },
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "ProjectProfilePermissionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "datazone:GetProjectProfile",
        "datazone:ListProjectProfiles"
      ],
      "Resource" : "arn:aws:datazone:*:*:domain/*"
    },
    {
      "Sid" : "AccountPoolPermissionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "datazone:GetAccountPool",
        "datazone:ListAccountPools",
```

```
        "datazone:ListAccountsInAccountPool"
      ],
      "Resource" : "arn:aws:datazone:*:*:domain/*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

SageMakerStudioDomainServiceRolePolicy

説明: Amazon SageMaker Studio が実行する、ポータルのドメインレベルのアクションのサービスロール。

SageMakerStudioDomainServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに SageMakerStudioDomainServiceRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2024 年 11 月 20 日 21:56 UTC
- 編集日時: 2024 年 11 月 20 日 21:56 UTC
- ARN: arn:aws:iam::aws:policy/service-role/SageMakerStudioDomainServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SSMGetParameterStatement",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/amazon/datazone/profiles/*"
      ]
    },
    {
      "Sid" : "UseKMSKeyPermissionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/EnableKeyForAmazonDataZone" : "true"
        },
        "Null" : {
          "aws:ResourceTag/EnableKeyForAmazonDataZone" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "ssm.*.amazonaws.com",
          "kms:EncryptionContext:PARAMETER_ARN" : "arn:aws:ssm:*:*:parameter/amazon/
datazone/profiles*"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

SageMakerStudioEMRContainersSystemNamespaceRolePolicy

説明: Amazon SageMaker Studio は、プロジェクトユーザーがデータ分析、人工知能、機械学習アクションを実行するための IAM ロールを作成し、これらのロールを作成して EMR に関連するアクセス許可を定義するときにこのポリシーを使用します。

SageMakerStudioEMRContainersSystemNamespaceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに SageMakerStudioEMRContainersSystemNamespaceRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2025 年 10 月 23 日 18:34 UTC
- 編集日時: 2025 年 10 月 30 日 20:34 UTC
- ARN: arn:aws:iam::aws:policy/service-role/SageMakerStudioEMRContainersSystemNamespaceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AssumeProjectRoles",
      "Effect" : "Allow",
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "TagSessionProjectRoles",
      "Effect" : "Allow",
      "Action" : [
        "sts:TagSession"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "LakeFormationAuthorizedCaller"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/LakeFormationAuthorizedCaller" : "EMR on EKS Engine",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
```

```
    {
      "Sid" : "SetContextProjectRoles",
      "Effect" : "Allow",
      "Action" : [
        "sts:SetContext"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*"
      ],
      "Condition" : {
        "ForAllValues:ArnEquals" : {
          "sts:RequestContextProviders" : [
            "arn:aws:iam::aws:contextProvider/IdentityCenter"
          ]
        },
        "Null" : {
          "sts:RequestContextProviders" : "false"
        },
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

SageMakerStudioEMRInstanceRolePolicy

説明: Amazon SageMaker Studio は、プロジェクトユーザーがデータ分析、人工知能、機械学習アクションを実行するための IAM ロールを作成し、これらのロールを作成して EMR に関連するアクセス許可を定義するときにこのポリシーを使用します。

SageMakerStudioEMRInstanceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに SageMakerStudioEMRInstanceRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2025 年 2 月 27 日 00:22 UTC
- 編集日時: 2025 年 2 月 27 日 00:22 UTC
- ARN: arn:aws:iam::aws:policy/service-role/SageMakerStudioEMRInstanceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AccessCertificateLocationS3Permission",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/certificate_location/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : ""
        },
        "Null" : {
```

```
          "aws:PrincipalTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AccessPatchingRPMsS3Permission",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : [
        "arn:aws:s3:::default-env-blueprint-*/*",
        "arn:aws:s3:*:*:accesspoint/env-blueprint-accesspoint*"
      ],
      "Condition" : {
        "ArnLike" : {
          "s3:DataAccessPointArn" : "arn:aws:s3:*:*:accesspoint/env-blueprint-
accesspoint"
        },
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AccessBootstrapActionScriptS3Permission",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/
${aws:PrincipalTag/AmazonDataZoneScopeName}/sys/emr/bootstrap-script/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : "",
          "aws:PrincipalTag/AmazonDataZoneScopeName" : ""
        },
        "Null" : {
          "aws:PrincipalTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Sid" : "EMRClusterLogUploadS3Permission",
      "Effect" : "Allow",
      "Action" : "s3:PutObject",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/
${aws:PrincipalTag/AmazonDataZoneScopeName}/sys/emr/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : "",
          "aws:PrincipalTag/AmazonDataZoneScopeName" : ""
        },
        "Null" : {
          "aws:PrincipalTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRRuntimeRoleAssumePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sts:AssumeRole",
        "sts:TagSession"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "LakeFormationAuthorizedCaller"
          ]
        },
        "StringEquals" : {
          "iam:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
```

```
    },
    {
      "Sid" : "EMRKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "AllowGenerateDataKeyForEbsEncryption",
      "Effect" : "Allow",
      "Action" : "kms:GenerateDataKey",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

SageMakerStudioEMRServiceRolePolicy

説明: Amazon SageMaker Studio は、プロジェクトユーザーがデータ分析、人工知能、機械学習アクションを実行するための IAM ロールを作成し、これらのロールを作成して EMR に関連するアクセス許可を定義するときにこのポリシーを使用します。

SageMakerStudioEMRServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに SageMakerStudioEMRServiceRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2025 年 1 月 31 日 19:52 UTC
- 編集日時: 2025 年 7 月 22 日 16:52 UTC
- ARN: arn:aws:iam::aws:policy/service-role/SageMakerStudioEMRServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "PassRoleToEMREC2InstanceRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/datazone_emr_ec2_instance_role_
${aws:PrincipalTag/AmazonDataZoneProject}_${aws:PrincipalTag/
AmazonDataZoneEnvironment}",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/AmazonDataZoneProject" : "",
          "aws:PrincipalTag/AmazonDataZoneEnvironment" : ""
        },
        "Null" : {
          "aws:PrincipalTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CreateInNetworkForSharedSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:RunInstances",
        "ec2:CreateFleet"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ArnLike" : {
          "ec2:Vpc" : "arn:aws:ec2:*:*:vpc/${aws:PrincipalTag/VpcId}"
        }
      }
    },
    {
      "Sid" : "EMRKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
```

```
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "AllowGenerateDataKeyForEbsEncryption",
      "Effect" : "Allow",
      "Action" : "kms:GenerateDataKey",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowDescribeKeyForLogPusherCMK",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
```

```
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

SageMakerStudioFullAccess

説明: このポリシーは、Amazon SageMaker マネジメントコンソールを介して Amazon SageMaker Unified Studio へのフルアクセスを提供します。

`SageMakerStudioFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `SageMakerStudioFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 11 月 28 日 00:06 UTC
- 編集日時: 2025 年 7 月 23 日 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonDataZoneStatement",
      "Effect" : "Allow",
      "Action" : [
        "datazone:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ReadOnlyStatement",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "iam:ListRoles",
        "iam:ListPolicies",
        "sso:DescribeRegisteredRegions",
        "s3:ListAllMyBuckets",
        "redshift:DescribeClusters",
        "redshift-serverless:ListWorkgroups",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "secretsmanager:ListSecrets",
        "iam:ListUsers",
        "glue:GetDatabases",
        "codeconnections:ListConnections",
        "codeconnections:ListTagsForResource",
        "codewhisperer:ListProfiles",
        "bedrock:ListInferenceProfiles",
        "bedrock:ListFoundationModels",
        "bedrock:ListTagsForResource",
        "aoss:ListSecurityPolicies",
        "quicksight:DescribeAccountSubscription",
        "cloudformation:ValidateTemplate"
      ],
```

```
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "BucketReadOnlyStatement",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:ListBucketVersions"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "ReadManagedBlueprintTemplatesStatement",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : [
        "arn:aws:s3:::default-env-blueprint-*/*",
        "arn:aws:s3:*:*:accesspoint/env-blueprint-accesspoint*"
      ],
      "Condition" : {
        "ArnLike" : {
          "s3:DataAccessPointArn" : "arn:aws:s3:*:*:accesspoint/env-blueprint-
accesspoint"
        },
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CreateBucketStatement",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::amazon-datazone*",
        "arn:aws:s3:::amazon-sagemaker*"
      ]
    },
    {
```

```
      "Sid" : "ConfigureBucketStatement",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketCORS",
        "s3:PutBucketPolicy",
        "s3:PutBucketVersioning"
      ],
      "Resource" : [
        "arn:aws:s3:::amazon-sagemaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "PutObjectStatement",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::amazon-sagemaker*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RamCreateResourceStatement",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "ram:RequestedResourceType" : "datazone:Domain"
        }
      }
```

```
    },
    {
      "Sid" : "RamResourceStatement",
      "Effect" : "Allow",
      "Action" : [
        "ram:DeleteResourceShare",
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare",
        "ram:RejectResourceShareInvitation"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ram:ResourceShareName" : [
            "DataZone*"
          ]
        }
      }
    },
    {
      "Sid" : "RamResourceReadOnlyStatement",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShares",
        "ram:GetResourceShareInvitations",
        "ram:GetResourceShareAssociations",
        "ram:ListResourceSharePermissions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RamAssociateResourceSharePermissionStatement",
      "Effect" : "Allow",
      "Action" : "ram:AssociateResourceSharePermission",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ram:PermissionArn" : [
            "arn:aws:ram::aws:permission/AWSRAMDefaultPermissionAmazonDataZoneDomain",
            "arn:aws:ram::aws:permission/
AWSRAMPermissionAmazonDataZoneDomainFullAccessWithPortalAccess",
            "arn:aws:ram::aws:permission/
AWSRAMPermissionsAmazonDatazoneDomainExtendedServiceAccess",
```

```
            "arn:aws:ram::aws:permission/
AWSRAMPermissionsAmazonDatazoneDomainExtendedServiceWithPortalAccess"
          ]
        }
      }
    },
    {
      "Sid" : "IAMPassRoleStatement",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/AmazonDataZone*",
        "arn:aws:iam::*:role/service-role/AmazonDataZone*",
        "arn:aws:iam::*:role/service-role/AmazonSageMaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:passedToService" : "datazone.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMGetPolicyStatement",
      "Effect" : "Allow",
      "Action" : "iam:GetPolicy",
      "Resource" : [
        "arn:aws:iam::*:policy/service-role/AmazonDataZoneRedshiftAccessPolicy*"
      ]
    },
    {
      "Sid" : "DataZoneTagOnCreateDomainProjectTags",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneDomain",
            "AmazonDataZoneProject"
          ]
        },
        "StringLike" : {
```

```
          "aws:RequestTag/AmazonDataZoneDomain" : "dzd*",
          "aws:ResourceTag/AmazonDataZoneDomain" : "dzd*"
        }
      }
    },
    {
      "Sid" : "DataZoneTagOnCreate",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneDomain"
          ]
        },
        "StringLike" : {
          "aws:RequestTag/AmazonDataZoneDomain" : "dzd*",
          "aws:ResourceTag/AmazonDataZoneDomain" : "dzd*"
        }
      }
    },
    {
      "Sid" : "CreateSecretStatement",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AmazonDataZoneDomain" : "dzd*"
        }
      }
    },
    {
      "Sid" : "ConnectionStatement",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:GetConnection"
      ],
      "Resource" : [
```

```
        "arn:aws:codeconnections:*:*:connection/*"
      ]
    },
    {
      "Sid" : "TagCodeConnectionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:TagResource"
      ],
      "Resource" : [
        "arn:aws:codeconnections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:host/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "for-use-with-all-datazone-projects"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "UntagCodeConnectionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:UntagResource"
      ],
      "Resource" : [
        "arn:aws:codeconnections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:host/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "for-use-with-all-datazone-projects"
        }
      }
    },
    {
      "Sid" : "SSMParameterStatement",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ssm:GetParameter",
        "ssm:GetParametersByPath",
        "ssm:PutParameter",
        "ssm:DeleteParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/amazon/datazone/q*",
        "arn:aws:ssm:*:*:parameter/amazon/datazone/genAI*",
        "arn:aws:ssm:*:*:parameter/amazon/datazone/profiles*"
      ]
    },
    {
      "Sid" : "UseKMSKeyPermissionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/EnableKeyForAmazonDataZone" : "true"
        },
        "Null" : {
          "aws:ResourceTag/EnableKeyForAmazonDataZone" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "ssm.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SecurityPolicyStatement",
      "Effect" : "Allow",
      "Action" : [
        "aoss:GetSecurityPolicy",
        "aoss:CreateSecurityPolicy"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
```

```
          "aoss:collection" : "bedrock-ide-*"
        }
      }
    },
    {
      "Sid" : "GetFoundationModelStatement",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetFoundationModel",
        "bedrock:GetFoundationModelAvailability"
      ],
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*"
      ]
    },
    {
      "Sid" : "GetInferenceProfileStatement",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetInferenceProfile"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:inference-profile/*",
        "arn:aws:bedrock:*:*:application-inference-profile/*"
      ]
    },
    {
      "Sid" : "ApplicationInferenceProfileStatement",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateInferenceProfile"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:application-inference-profile/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AmazonDataZoneProject" : "true",
          "aws:RequestTag/AmazonDataZoneDomain" : "false"
        }
      }
    },
    {
      "Sid" : "TagApplicationInferenceProfileStatement",
```

```
      "Effect" : "Allow",
      "Action" : [
        "bedrock:TagResource"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:application-inference-profile/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "true",
          "aws:RequestTag/AmazonDataZoneProject" : "true",
          "aws:ResourceTag/AmazonDataZoneDomain" : "false",
          "aws:RequestTag/AmazonDataZoneDomain" : "false"
        }
      }
    },
    {
      "Sid" : "DeleteApplicationInferenceProfileStatement",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:DeleteInferenceProfile"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:application-inference-profile/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "true",
          "aws:ResourceTag/AmazonDataZoneDomain" : "false"
        }
      }
    },
    {
      "Sid" : "ModelAccessUseCaseStatement",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetUseCaseForModelAccess",
        "bedrock:PutUseCaseForModelAccess"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
```

```
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

SageMakerStudioProjectProvisioningRolePolicy

説明: Amazon SageMaker Studio は、このポリシーを使用してアカウントのリソースをプロビジョニングおよび管理します。

`SageMakerStudioProjectProvisioningRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `SageMakerStudioProjectProvisioningRolePolicy` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2024 年 11 月 20 日 21:58 UTC
- 編集日時: 2025 年 11 月 21 日 00:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioProjectProvisioningRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v24 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CfnCreate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:TagResource"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        }
      }
    },
    {
      "Sid" : "CfnManage",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:UpdateStack"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "CfnDelete",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ValidateCfn",
      "Effect" : "Allow",
      "Action" : "cloudformation:ValidateTemplate",
      "Resource" : "*"
    },
    {
      "Sid" : "LFManage",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataLakeSettings",
        "lakeformation:PutDataLakeSettings",
        "lakeformation:RevokePermissions",
        "lakeformation:BatchRevokePermissions",
        "lakeformation:ListPermissions",
        "lakeformation:RegisterResource",
        "lakeformation:DeregisterResource",
        "lakeformation:GrantPermissions",
        "lakeformation:BatchGrantPermissions",
        "lakeformation:ListResources",
        "lakeformation:DescribeResource",
```

```
        "lakeformation:*LakeFormationIdentityCenterConfiguration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DzTemplate",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DzCfTemplate",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::amazon-sagemaker-cf-templates*/*"
    },
    {
      "Sid" : "CcCreate",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:CreateRepository",
        "codecommit:TagResource"
      ],
      "Resource" : "arn:aws:codecommit:*:*:datazone*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "CcDelete",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:DeleteRepository",
        "codecommit:UntagResource",
        "codecommit:UpdateRepositoryEncryptionKey",
        "codecommit:PutRepositoryTriggers"
      ],
      "Resource" : "arn:aws:codecommit:*:*:datazone*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "CcAccess",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:GetBranch",
        "codecommit:CreateCommit",
        "codecommit:GetRepository",
        "codecommit:GetFile"
      ],
      "Resource" : "arn:aws:codecommit:*:*:datazone*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CcList",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:ListRepositories"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "CcKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "codecommit.*.amazonaws.com"
          ]
        },
        "Null" : {
          "kms:EncryptionContext:aws:codecommit:id" : "false"
        }
      }
    },
    {
      "Sid" : "GetIamRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*",
        "arn:aws:iam::*:role/AmazonBedrock*",
        "arn:aws:iam::*:role/BedrockStudio*"
      ]
    },
    {
      "Sid" : "IAMManage",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:DetachRolePolicy",
```

```
        "iam:DeleteRolePolicy",
        "iam:AttachRolePolicy",
        "iam:PutRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*",
        "arn:aws:iam::*:role/AmazonBedrockExecution*",
        "arn:aws:iam::*:role/BedrockStudio*",
        "arn:aws:iam::*:role/AmazonBedrockConsumptionRole*",
        "arn:aws:iam::*:role/AmazonBedrockEvaluation*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/
SageMakerStudioProjectUserRolePermissionsBoundary"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "IamDzManage",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRolePolicy",
        "iam:PutRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/
SageMakerStudioProjectUserRolePermissionsBoundary"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "RoleCreate",
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:CreateRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*",
        "arn:aws:iam::*:role/AmazonBedrock*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "IamManage",
      "Effect" : "Allow",
      "Action" : [
        "iam:DetachRolePolicy",
        "iam:AttachRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/SageMakerStudioProjectUserRolePolicy",
            "arn:aws:iam::aws:policy/SageMakerStudioProjectRoleMachineLearningPolicy",
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioEMRContainersSystemNamespaceRolePolicy",
            "arn:aws:iam::aws:policy/service-role/SageMakerStudioEMRServiceRolePolicy",
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioEMRInstanceRolePolicy",
            "arn:aws:iam::aws:policy/service-role/AmazonEMRServicePolicy_v2",
            "arn:aws:iam::aws:policy/service-role/
AmazonS3TablesLakeFormationServiceRole",
            "arn:aws:iam::aws:policy/AmazonSageMakerPartnerAppsFullAccess",
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "IamManageAdmin",
      "Effect" : "Allow",
      "Action" : [
        "iam:DetachRolePolicy",
        "iam:AttachRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneAdminProject" : "false"
        },
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/SageMakerStudioAdminProjectUserRolePolicy"
          ]
        }
      }
    },
    {
      "Sid" : "IamManageBR",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/AmazonBedrock*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole",
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioBedrockAgentServiceRolePolicy",
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioBedrockChatAgentUserRolePolicy",
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioBedrockFlowServiceRolePolicy",
```

```
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioBedrockFunctionExecutionRolePolicy",
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy",
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioBedrockKnowledgeBaseCustomResourcePolicy",
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioBedrockPromptUserRolePolicy",
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioBedrockEvaluationJobServiceRolePolicy"
          ]
        }
      }
    },
    {
      "Sid" : "IamTag",
      "Effect" : "Allow",
      "Action" : [
        "iam:TagRole",
        "iam:UntagRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*",
        "arn:aws:iam::*:role/datazone_s3tables_*",
        "arn:aws:iam::*:role/datazone-partner-apps-*",
        "arn:aws:iam::*:role/datazone_redshift_serverless_admin_role_*",
        "arn:aws:iam::*:role/AmazonBedrock*",
        "arn:aws:iam::*:role/BedrockStudio*",
        "arn:aws:iam::*:role/SageMakerStudioQueryExecutionRole"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "BootstrappedServices",
            "AmazonBedrockManaged",
            "RedshiftDb*",
            "EnableAmazonBedrockPermissions",
            "EnableAmazonBedrockIDEPermissions",
            "EnableGlueWorkloadsPermissions",
```

```
            "EnableSageMakerMLWorkloadsPermissions",
            "DomainBucketName",
            "KmsKeyId",
            "DomainKmsKeyId",
            "DefaultGlueCatalogKmsKeyId",
            "LogGroupName",
            "RoleName",
            "vpcArn",
            "VpcId",
            "CreatedForUseWithSageMakerStudio",
            "SageMakerStudioQueryExecutionRole"
          ]
        }
      }
    },
    {
      "Sid" : "AdminProjectTagRoleManagement",
      "Effect" : "Allow",
      "Action" : [
        "iam:TagRole",
        "iam:UntagRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZoneScopeName",
            "BootstrappedServices",
            "AmazonDataZoneAdminProject"
          ]
        }
      }
    },
    {
      "Sid" : "IamTagBR",
      "Effect" : "Allow",
      "Action" : [
        "iam:TagRole",
        "iam:UntagRole"
```

```
      ],
      "Resource" : "arn:aws:iam::*:role/AmazonBedrock*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "AmazonBedrockManaged",
            "DomainBucketName",
            "KmsKeyId",
            "AgentId",
            "AgentAliasId",
            "AppDefinitionPath",
            "DataSourcePath",
            "PromptId",
            "PromptVersion",
            "PromptDefinitionPath",
            "OpenSearchServerlessCollectionId"
          ]
        }
      }
    },
    {
      "Sid" : "IamTagRS",
      "Effect" : "Allow",
      "Action" : "iam:TagRole",
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "RedshiftDb*"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "IamTagEMR",
      "Effect" : "Allow",
      "Action" : [
        "iam:TagRole",
        "iam:UntagRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone_emr_service_role_*",
        "arn:aws:iam::*:role/datazone_emr_ec2_instance_role_*",
        "arn:aws:iam::*:role/datazone_emr_containers_system_namespace_role_*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "DataZone*",
            "for-use-with-amazon-emr-managed-policies",
            "DomainBucketName",
            "KmsKeyId",
            "VpcId"
          ]
        }
      }
    },
    {
      "Sid" : "IamUntag",
      "Effect" : "Allow",
      "Action" : "iam:UntagRole",
      "Resource" : "arn:aws:iam::*:role/datazone_usr_role_*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "EnableAmazonBedrockIDEPermissions"
        }
      }
    },
    {
      "Sid" : "ManageRoles",
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole",
        "iam:DeleteRolePolicy",
        "iam:ListRolePolicies",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*",
        "arn:aws:iam::*:role/AmazonBedrock*",
        "arn:aws:iam::*:role/BedrockStudio*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "DzManageRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:UpdateAssumeRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*",
        "arn:aws:iam::*:role/datazone_emr_*",
        "arn:aws:iam::*:role/datazone-partner-apps-*",
        "arn:aws:iam::*:role/AmazonBedrock*",
        "arn:aws:iam::*:role/datazone_s3tables_*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "IamAttach",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy"
```

```
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/
SageMakerStudioProjectUserRolePermissionsBoundary"
        }
      }
    },
    {
      "Sid" : "IamDetach",
      "Effect" : "Allow",
      "Action" : [
        "iam:DetachRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*",
        "arn:aws:iam::*:role/AmazonBedrock*"
      ]
    },
    {
      "Sid" : "DzManagePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeletePolicy",
        "iam:CreatePolicy",
        "iam:ListPolicies",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:CreatePolicyVersion",
        "iam:ListPolicyVersions",
        "iam:DeletePolicyVersion"
      ],
      "Resource" : [
        "arn:aws:iam::*:policy/datazone*",
        "arn:aws:iam::*:policy/connector-manage-access-policy*",
        "arn:aws:iam::*:policy/SageMakerStudioQueryExecutionRolePolicy"
      ]
    },
    {
      "Sid" : "ListPolicy",
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:ListPolicies"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueConnection",
      "Effect" : "Allow",
      "Action" : [
        "glue:ListConnectionTypes",
        "glue:DescribeConnectionType",
        "glue:*GlueIdentityCenterConfiguration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "InstanceProfile",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile",
        "iam:CreateInstanceProfile",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteInstanceProfile"
      ],
      "Resource" : "arn:aws:iam::*:instance-profile/
datazone_emr_ec2_instance_profile_*"
    },
    {
      "Sid" : "PassRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*",
        "arn:aws:iam::*:role/SageMakerStudioQueryExecutionRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com",
            "glue.amazonaws.com"
          ],
          "iam:PassedToService" : [
            "glue.amazonaws.com",
```

```
            "lakeformation.amazonaws.com",
            "redshift-serverless.amazonaws.com",
            "redshift.amazonaws.com",
            "emr-serverless.amazonaws.com",
            "airflow.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PassRoleForDZ",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com",
            "redshift-serverless.amazonaws.com",
            "bedrock.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PassRoleForGlue",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*",
        "arn:aws:iam::*:role/datazone_s3tables_*",
        "arn:aws:iam::*:role/SageMakerStudioQueryExecutionRole",
        "arn:aws:iam::*:role/service-role/AmazonSageMakerQueryExecution"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com",
            "lakeformation.amazonaws.com"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "PassRoleForEmr",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/datazone_emr_service_role_*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "elasticmapreduce.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PassRoleForEmrIP",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/datazone_emr_ec2_instance_role_*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PassRoleToBR",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/AmazonBedrock*",
        "arn:aws:iam::*:role/BedrockStudio*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "bedrock.amazonaws.com"
        }
      }
```

```
    },
    {
      "Sid" : "PassRoleToLambda",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/AmazonBedrock*",
        "arn:aws:iam::*:role/BedrockStudio*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AossSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
observability.aoss.amazonaws.com/AWSServiceRoleForAmazonOpenSearchServerless",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "observability.aoss.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "GlueDb",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:GetDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:database/default",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/s3tablescatalog",
        "arn:aws:glue:*:*:catalog/s3tablescatalog/*",
        "arn:aws:glue:*:*:database/s3tablescatalog/*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Sid" : "CfnGlueDb",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:database/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueDbTag",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:catalog"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueDbDelete",
      "Effect" : "Allow",
      "Action" : [
        "glue:DeleteDatabase"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Sid" : "GlueTag",
      "Effect" : "Allow",
      "Action" : [
        "glue:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        }
      }
    },
    {
      "Sid" : "GlueConnTag",
      "Effect" : "Allow",
      "Action" : "glue:GetConnection",
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:connection/datazone-glue-network-connection-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueConnManage",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateConnection",
        "glue:DeleteConnection"
```

```
      ],
      "Resource" : [
        "arn:aws:glue:*:*:connection/datazone-glue-network-connection-*",
        "arn:aws:glue:*:*:catalog"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueConnections",
      "Action" : [
        "glue:PassConnection",
        "glue:GetConnections",
        "glue:GetTags"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:connection/*",
        "arn:aws:glue:*:*:catalog/*"
      ],
      "Effect" : "Allow",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "AthenaConnection",
      "Action" : [
        "athena:CreateDataCatalog"
      ],
      "Resource" : "*",
      "Effect" : "Allow",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "GetConnection",
```

```
      "Effect" : "Allow",
      "Action" : [
        "glue:GetConnection"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:connection/*",
        "arn:aws:glue:*:*:catalog/*"
      ]
    },
    {
      "Sid" : "ConnectionTag",
      "Effect" : "Allow",
      "Action" : [
        "athena:TagResource"
      ],
      "Resource" : "arn:aws:athena:*:*:datacatalog/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "federated_athena*"
          ]
        }
      }
    },
    {
      "Sid" : "CreateConn",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateConnection"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:connection/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
```

```
          "aws:RequestTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "ManageConnection",
      "Effect" : "Allow",
      "Action" : [
        "glue:DeleteConnection",
        "glue:UpdateConnection"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:connection/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "ManageCatalogConn",
      "Effect" : "Allow",
      "Action" : [
        "glue:DeleteConnection",
        "glue:UpdateConnection"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
```

```
        "kms:Encrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "kms:EncryptionContext:glue_catalog_id" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "glue.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "GetDataCatalogEncSett",
      "Action" : "glue:GetDataCatalogEncryptionSettings",
      "Effect" : "Allow",
      "Resource" : "arn:aws:glue:*:*:catalog",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "Repo",
      "Effect" : "Allow",
      "Action" : [
        "serverlessrepo:GetCloudFormationTemplate",
        "serverlessrepo:CreateCloudFormationTemplate"
      ],
      "Resource" : [
        "arn:aws:serverlessrepo:*:*:applications/Athena*"
      ]
    },
    {
      "Sid" : "Ecr",
      "Effect" : "Allow",
      "Action" : [
        "imagebuilder:GetComponent",
        "imagebuilder:GetContainerRecipe",
```

```
        "ecr:GetAuthorizationToken",
        "ecr:BatchGetImage",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/athena-federation-repository*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "lambda.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CfnChangeSet",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:DeleteChangeSet"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:transform/Serverless*"
      ]
    },
    {
      "Sid" : "LambdaManage",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:DeleteFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:athenafederatedcatalog*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
```

```
    {
      "Sid" : "LambdaGet",
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:athenafederatedcatalog*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:CalledViaLast" : [
            "athena.amazonaws.com",
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "LambdaUpdate",
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetFunctionConfiguration",
        "lambda:UpdateFunctionConfiguration"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:athenafederatedcatalog*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "TagLambda",
      "Effect" : "Allow",
      "Action" : [
        "lambda:TagResource"
      ],
```

```
      "Resource" : [
        "arn:aws:lambda:*:*:function:athenafederatedcatalog*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "aws:cloudformation:*",
            "federated_athena*",
            "lambda:createdBy"
          ]
        }
      }
    },
    {
      "Sid" : "LambdaS3Get",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::awsserverlessrepo*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:CalledViaLast" : [
            "lambda.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "S3List",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
```

```
      "Resource" : [
        "arn:aws:s3:::*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "s3:prefix" : "true"
        }
      }
    },
    {
      "Sid" : "S3Create",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutBucketTagging",
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketCORS",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketPolicy",
        "s3:DeleteBucketPolicy",
        "s3:GetBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-*"
      ]
    },
    {
      "Sid" : "Cfn",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/athenafederatedcatalog*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/federated_athena_datacatalog" : "false"
        }
      }
```

```
    },
    {
      "Sid" : "AthenaDC",
      "Effect" : "Allow",
      "Action" : [
        "athena:DeleteDataCatalog",
        "athena:GetDataCatalog",
        "athena:UpdateDataCatalog"
      ],
      "Resource" : "arn:aws:athena:*:*:datacatalog/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "LambdaPassRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lambda.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "GetRole",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/SageMakerStudioQueryExecutionRole",
        "arn:aws:iam::*:role/service-role/AmazonSageMakerQueryExecution",
        "arn:aws:iam::*:role/datazone_s3tables_*"
      ],
      "Effect" : "Allow"
    },
    {
```

```
      "Sid" : "S3tPassConn",
      "Effect" : "Allow",
      "Action" : [
        "glue:PassConnection"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:connection/aws:s3tables"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "LFAccess",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "lakeformation:EnabledOnlyForMetaDataAccess" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueCatalogCreate",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateCatalog"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:RequestTag/AmazonDataZoneProject" : "false"
```

```
        }
      }
    },
    {
      "Sid" : "GlueCatalogMgmt",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetCatalog",
        "glue:GetCatalogs",
        "glue:UpdateCatalog",
        "glue:DeleteCatalog",
        "glue:GetDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RSManage",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:CreateNamespace",
        "redshift-serverless:CreateWorkgroup",
        "redshift-serverless:DeleteNamespace",
        "redshift-serverless:DeleteWorkgroup",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:ListSnapshotCopyConfigurations",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*",
        "arn:aws:redshift-serverless:*:*:workgroup/*",
        "arn:aws:redshift-serverless:*:*:snapshotcopyconfiguration/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Sid" : "RedshiftDataShare",
      "Effect" : "Allow",
      "Action" : [
        "redshift:AssociateDataShareConsumer",
        "redshift:AuthorizeDataShare"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:datashare:*/*"
      ],
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : [
            "redshift-serverless.amazonaws.com",
            "glue.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RedshiftBucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:PutBucketPolicy",
        "s3:PutEncryptionConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketVersioning",
        "s3:PutBucketTagging"
      ],
      "Resource" : "arn:aws:s3:::redshift-staging-bucket-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
```

```
    {
      "Sid" : "RedshiftTag",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:TagResource"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*",
        "arn:aws:redshift-serverless:*:*:workgroup/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        }
      }
    },
    {
      "Sid" : "CreateSG",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:TagKeys" : "true"
        }
      }
    },
    {
      "Sid" : "SGAuth",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "SGManage",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "SGRevoke",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "TagEc2",
```

```
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "for-use-with-amazon-emr-managed-policies",
            "aws:cloudformation:*"
          ]
        }
      }
    },
    {
      "Sid" : "EC2Describe",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeNatGateways",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeLG",
      "Effect" : "Allow",
      "Action" : "logs:DescribeLogGroups",
      "Resource" : "*"
    },
    {
      "Sid" : "CreateLG",
      "Effect" : "Allow",
```

```
      "Action" : [
        "logs:CreateLogGroup",
        "logs:TagResource"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:datazone-*",
        "arn:aws:logs:*:*:log-group:/aws/lambda/amazon-bedrock-ide-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "AmazonBedrockManaged"
          ]
        }
      }
    },
    {
      "Sid" : "LGRetention",
      "Effect" : "Allow",
      "Action" : "logs:PutRetentionPolicy",
      "Resource" : [
        "arn:aws:logs:*:*:log-group:datazone-*",
        "arn:aws:logs:*:*:log-group:/aws/lambda/amazon-bedrock-ide-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ManageLG",
      "Effect" : "Allow",
      "Action" : [
        "logs:DeleteLogGroup",
        "logs:UntagResource",
        "logs:DeleteRetentionPolicy",
```

```
        "logs:GetDataProtectionPolicy",
        "logs:PutDataProtectionPolicy",
        "logs:DeleteDataProtectionPolicy",
        "logs:AssociateKmsKey",
        "logs:DisassociateKmsKey",
        "logs:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:datazone-*",
        "arn:aws:logs:*:*:log-group:/aws/lambda/amazon-bedrock-ide-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "AthenaManage",
      "Effect" : "Allow",
      "Action" : [
        "athena:CreateWorkGroup",
        "athena:TagResource"
      ],
      "Resource" : "arn:aws:athena:*:*:workgroup/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "AthenaWGDelete",
      "Effect" : "Allow",
      "Action" : [
        "athena:DeleteWorkGroup",
        "athena:UpdateWorkGroup",
        "athena:UntagResource",
        "athena:GetWorkGroup"
      ],
      "Resource" : "arn:aws:athena:*:*:workgroup/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "RedshiftCreate",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:CreateNamespace",
        "redshift-serverless:CreateWorkgroup",
        "redshift-serverless:TagResource"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*",
        "arn:aws:redshift-serverless:*:*:workgroup/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "TagRSS",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*",
        "arn:aws:redshift-serverless:*:*:workgroup/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ManageSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:UpdateSecret"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:ResourceTag/CreatedBy" : "false"
        }
      }
    },
    {
      "Sid" : "SecretProject",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
```

```
        }
      }
    },
    {
      "Sid" : "SecretAll",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "TagSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:ResourceTag/CreatedBy" : "false",
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "CreatedBy"
          ]
        }
      }
    },
    {
      "Sid" : "SecretKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
```

```
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "secretsmanager.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContext:SecretARN" : "false"
        }
      }
    },
    {
      "Sid" : "CreateSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/neptune-graph.amazonaws.com/
AWSServiceRoleForNeptuneGraph",
        "arn:aws:iam::*:role/aws-service-role/redshift.amazonaws.com/
AWSServiceRoleForRedshift",
        "arn:aws:iam::*:role/aws-service-role/sagemaker.amazonaws.com/
AWSServiceRoleForAmazonSageMakerNotebooks",
        "arn:aws:iam::*:role/aws-service-role/ops.emr-serverless.amazonaws.com/
AWSServiceRoleForAmazonEMRServerless",
        "arn:aws:iam::*:role/aws-service-role/airflow.amazonaws.com/
AWSServiceRoleForAmazonMWAA",
        "arn:aws:iam::*:role/aws-service-role/elasticmapreduce.amazonaws.com/
AWSServiceRoleForEMRCleanup",
        "arn:aws:iam::*:role/aws-service-role/emr-containers.amazonaws.com/
AWSServiceRoleForAmazonEMRContainers"
      ]
    },
    {
      "Sid" : "RedshiftList",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
```

```
        "redshift:GetResourcePolicy"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RssDbRole",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:ExecuteStatement",
        "redshift:GetResourcePolicy",
        "redshift-serverless:GetCredentials"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*",
        "arn:aws:redshift-serverless:*:*:workgroup/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "RedshiftData",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:DescribeStatement",
        "redshift-data:GetStatementResult",
        "redshift:DescribeDataSharesForConsumer",
        "redshift:DescribeDataShares"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftManage",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:UpdateNamespace",
        "redshift-serverless:UpdateWorkgroup",
        "redshift-serverless:UntagResource"
      ],
```

```
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*",
        "arn:aws:redshift-serverless:*:*:workgroup/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "RedshiftKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "redshift-serverless.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContext:aws:redshift-serverless:arn" : "false"
        }
      }
    },
    {
      "Sid" : "GetRandom",
      "Effect" : "Allow",
      "Action" : "secretsmanager:GetRandomPassword",
      "Resource" : "*"
    },
    {
      "Sid" : "BRSecret",
```

```
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:CreateSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:PutResourcePolicy",
        "secretsmanager:DeleteResourcePolicy",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:amazon-bedrock-ide/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "RedshiftSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:RotateSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DeleteSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:redshift!*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagRsSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource"
      ],
```

```
      "Resource" : "arn:aws:secretsmanager:*:*:secret:redshift!*",
      "Condition" : {
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "Redshift",
            "aws:secretsmanager:*",
            "aws:redshift-serverless:*",
            "AmazonDataZone*",
            "datazone.rs.workgroup"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagSMD",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:domain/*",
        "arn:aws:sagemaker:*:*:mlflow-tracking-server/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "TagSMDForUpdate",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateDomain",
        "sagemaker:AddTags"
```

```
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:domain/*",
        "arn:aws:sagemaker:*:*:mlflow-tracking-server/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:RequestTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "ManageSMD",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:UpdateDomain",
        "sagemaker:DeleteDomain"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:domain/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "SMDManage",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListDomains",
        "sagemaker:DescribeDomain"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SMAppDelete",
      "Effect" : "Allow",
      "Action" : "sagemaker:DeleteApp",
```

```
      "Resource" : [
        "arn:aws:sagemaker:*:*:app/*/*/codeeditor/*",
        "arn:aws:sagemaker:*:*:app/*/*/CodeEditor/*",
        "arn:aws:sagemaker:*:*:app/*/*/jupyterlab/*",
        "arn:aws:sagemaker:*:*:app/*/*/JupyterLab/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "DeleteSpace",
      "Effect" : "Allow",
      "Action" : "sagemaker:DeleteSpace",
      "Resource" : "arn:aws:sagemaker:*:*:space/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "DeleteUserProfile",
      "Effect" : "Allow",
      "Action" : "sagemaker:DeleteUserProfile",
      "Resource" : "arn:aws:sagemaker:*:*:user-profile/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
```

```
      "Sid" : "EmrSCreate",
      "Effect" : "Allow",
      "Action" : [
        "emr-serverless:CreateApplication",
        "emr-serverless:TagResource"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        }
      }
    },
    {
      "Sid" : "EmrSManage",
      "Effect" : "Allow",
      "Action" : [
        "emr-serverless:UpdateApplication",
        "emr-serverless:DeleteApplication"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
```

```
      "Sid" : "EmrSGetStop",
      "Effect" : "Allow",
      "Action" : [
        "emr-serverless:GetApplication",
        "emr-serverless:StopApplication"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "EmrSEc2Eni",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "ops.emr-serverless.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EmrSEc2Subnet",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "ops.emr-serverless.amazonaws.com"
        }
```

```
      }
    },
    {
      "Sid" : "MLFlowCreate",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateMlflowTrackingServer",
        "sagemaker:AddTags"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:mlflow-tracking-server/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:RequestTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "MLFlowDescribe",
      "Effect" : "Allow",
      "Action" : "sagemaker:DescribeMlflowTrackingServer",
      "Resource" : "arn:aws:sagemaker:*:*:mlflow-tracking-server/*"
    },
    {
      "Sid" : "MLFlowDelete",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DeleteMlflowTrackingServer"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:mlflow-tracking-server/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "AossManage",
      "Effect" : "Allow",
```

```
      "Action" : [
        "aoss:GetAccessPolicy",
        "aoss:CreateAccessPolicy",
        "aoss:DeleteAccessPolicy",
        "aoss:UpdateAccessPolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "aoss:collection" : "bedrock-ide-*",
          "aoss:index" : "bedrock-ide-*"
        }
      }
    },
    {
      "Sid" : "ManageAossPolicies",
      "Effect" : "Allow",
      "Action" : [
        "aoss:GetSecurityPolicy",
        "aoss:CreateSecurityPolicy",
        "aoss:DeleteSecurityPolicy",
        "aoss:UpdateSecurityPolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "aoss:collection" : "bedrock-ide-*"
        }
      }
    },
    {
      "Sid" : "GetAoss",
      "Effect" : "Allow",
      "Action" : "aoss:BatchGetCollection",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AossCollections",
      "Effect" : "Allow",
```

```
      "Action" : [
        "aoss:CreateCollection",
        "aoss:UpdateCollection",
        "aoss:DeleteCollection",
        "aoss:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "ManageNeptune",
      "Effect" : "Allow",
      "Action" : [
        "neptune-graph:CreateGraph",
        "neptune-graph:UpdateGraph",
        "neptune-graph:DeleteGraph",
        "neptune-graph:ListGraphs",
        "neptune-graph:GetGraph"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "S3VectorsManage",
      "Effect" : "Allow",
      "Action" : [
        "s3vectors:CreateVectorBucket",
        "s3vectors:DeleteVectorBucket",
        "s3vectors:ListVectorBuckets",
        "s3vectors:GetVectorBucket",
        "s3vectors:CreateIndex",
        "s3vectors:DeleteIndex",
        "s3vectors:ListIndexes",
```

```
        "s3vectors:GetIndex"
      ],
      "Resource" : "arn:aws:s3vectors:*:*:bucket/amazon-bedrock-ide-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagNeptune",
      "Effect" : "Allow",
      "Action" : [
        "neptune-graph:TagResource"
      ],
      "Resource" : "arn:aws:neptune-graph:*:*:graph/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "AmazonBedrock*"
          ]
        }
      }
    },
    {
      "Sid" : "GetS3GenAI",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::*/dzd*/*/genAI/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GetBR",
```

```
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetAgent",
        "bedrock:GetKnowledgeBase",
        "bedrock:GetGuardrail",
        "bedrock:GetPrompt",
        "bedrock:GetFlow",
        "bedrock:GetFlowAlias",
        "bedrock:ListTagsForResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BRManage",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateAgent",
        "bedrock:UpdateAgent",
        "bedrock:PrepareAgent",
        "bedrock:DeleteAgent",
        "bedrock:ListAgentAliases",
        "bedrock:GetAgentAlias",
        "bedrock:CreateAgentAlias",
        "bedrock:UpdateAgentAlias",
        "bedrock:DeleteAgentAlias",
        "bedrock:ListAgentActionGroups",
        "bedrock:GetAgentActionGroup",
        "bedrock:CreateAgentActionGroup",
        "bedrock:UpdateAgentActionGroup",
        "bedrock:DeleteAgentActionGroup",
        "bedrock:ListAgentKnowledgeBases",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:AssociateAgentKnowledgeBase",
        "bedrock:DisassociateAgentKnowledgeBase",
        "bedrock:UpdateAgentKnowledgeBase",
        "bedrock:CreateKnowledgeBase",
        "bedrock:UpdateKnowledgeBase",
        "bedrock:DeleteKnowledgeBase",
        "bedrock:ListDataSources",
```

```
        "bedrock:GetDataSource",
        "bedrock:CreateDataSource",
        "bedrock:UpdateDataSource",
        "bedrock:DeleteDataSource",
        "bedrock:ListIngestionJobs",
        "bedrock:GetIngestionJob",
        "bedrock:StartIngestionJob",
        "bedrock:StopIngestionJob",
        "bedrock:CreateGuardrail",
        "bedrock:UpdateGuardrail",
        "bedrock:DeleteGuardrail",
        "bedrock:CreateGuardrailVersion",
        "bedrock:CreatePrompt",
        "bedrock:UpdatePrompt",
        "bedrock:DeletePrompt",
        "bedrock:CreatePromptVersion",
        "bedrock:CreateFlow",
        "bedrock:UpdateFlow",
        "bedrock:PrepareFlow",
        "bedrock:DeleteFlow",
        "bedrock:ListFlowAliases",
        "bedrock:GetFlowAlias",
        "bedrock:CreateFlowAlias",
        "bedrock:UpdateFlowAlias",
        "bedrock:DeleteFlowAlias",
        "bedrock:ListFlowVersions",
        "bedrock:GetFlowVersion",
        "bedrock:CreateFlowVersion",
        "bedrock:DeleteFlowVersion",
        "bedrock:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "TagBR",
      "Effect" : "Allow",
```

```
      "Action" : "bedrock:TagResource",
      "Resource" : [
        "arn:aws:bedrock:*:*:agent-alias/*/TSTALIASID",
        "arn:aws:bedrock:*:*:flow/*/alias/TSTALIASID"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:RequestTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "ListBRJobs",
      "Effect" : "Allow",
      "Action" : "bedrock:ListEvaluationJobs",
      "Resource" : "*"
    },
    {
      "Sid" : "ManageBRJobs",
      "Effect" : "Allow",
      "Action" : "bedrock:BatchDeleteEvaluationJob",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "BRLambda",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:InvokeFunction",
        "lambda:DeleteFunction",
        "lambda:UpdateFunctionCode",
        "lambda:GetFunctionConfiguration",
        "lambda:UpdateFunctionConfiguration",
```

```
        "lambda:ListVersionsByFunction",
        "lambda:PublishVersion",
        "lambda:GetPolicy",
        "lambda:AddPermission",
        "lambda:TagResource"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:amazon-bedrock-ide-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "ManageBRLambda",
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetFunction",
        "lambda:ListTags",
        "lambda:RemovePermission"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:amazon-bedrock-ide-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRManage",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:CreateSecurityConfiguration",
        "elasticmapreduce:DeleteSecurityConfiguration",
        "elasticmapreduce:DescribeSecurityConfiguration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EMRClusterManage",
      "Effect" : "Allow",
```

```
      "Action" : [
        "elasticmapreduce:AddJobFlowSteps",
        "elasticmapreduce:AddTags",
        "elasticmapreduce:DescribeJobFlows",
        "elasticmapreduce:ListInstanceFleets",
        "elasticmapreduce:ModifyInstanceFleet",
        "elasticmapreduce:RunJobFlow",
        "elasticmapreduce:SetTerminationProtection",
        "elasticmapreduce:TerminateJobFlows",
        "elasticmapreduce:DescribeCluster"
      ],
      "Resource" : "arn:aws:elasticmapreduce:*:*:cluster/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "AirflowEnv",
      "Effect" : "Allow",
      "Action" : [
        "airflow:CreateEnvironment",
        "airflow:UpdateEnvironment",
        "airflow:DeleteEnvironment",
        "airflow:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "AirflowGet",
      "Effect" : "Allow",
      "Action" : [
        "airflow:GetEnvironment"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AirflowS3",
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:GetEncryptionConfiguration"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "VpcCreate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "ENICreate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    },
    {
      "Sid" : "KmsCreate",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "airflow.*.amazonaws.com",
            "neptune-graph.*.amazonaws.com",
            "s3vectors.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "KmsDescribe",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "QueryRoleManage",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:CreateRole",
        "iam:DetachRolePolicy",
        "iam:DeleteRolePolicy",
        "iam:AttachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/SageMakerStudioQueryExecutionRole",
      "Condition" : {
        "StringEquals" : {
          "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/
SageMakerStudioProjectUserRolePermissionsBoundary"
```

```
        }
      }
    },
    {
      "Sid" : "QueryRoleCreate",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole"
      ],
      "Resource" : "arn:aws:iam::*:role/SageMakerStudioQueryExecutionRole"
    },
    {
      "Sid" : "QueryRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:DetachRolePolicy",
        "iam:AttachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/SageMakerStudioQueryExecutionRole",
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioQueryExecutionRolePolicy"
          ]
        }
      }
    },
    {
      "Sid" : "TagQueryRole",
      "Effect" : "Allow",
      "Action" : "iam:TagRole",
      "Resource" : "arn:aws:iam::*:role/SageMakerStudioQueryExecutionRole",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "CreatedForUseWithSageMakerStudio",
            "SageMakerStudioQueryExecutionRole"
          ]
        }
      }
    },
    {
      "Sid" : "ListQueryPolicy",
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : "arn:aws:iam::*:role/SageMakerStudioQueryExecutionRole"
    },
    {
      "Sid" : "EMRCleanup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "EmrRoleCleanup",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:ListInstanceProfilesForRole",
        "iam:DeleteRolePolicy",
        "iam:DeleteRole"
      ],
      "Resource" : "arn:aws:iam::*:role/datazone_emr_*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "EmrInstanceCleanup",
      "Effect" : "Allow",
      "Action" : [
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteInstanceProfile"
      ],
```

```
      "Resource" : "arn:aws:iam::*:instance-profile/
datazone_emr_ec2_instance_profile_*"
    },
    {
      "Sid" : "Scheduler",
      "Effect" : "Allow",
      "Action" : [
        "scheduler:ListTagsForResource",
        "scheduler:GetScheduleGroup"
      ],
      "Resource" : "arn:aws:scheduler:*:*:schedule-group/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ScheduleGroup",
      "Effect" : "Allow",
      "Action" : [
        "scheduler:DeleteScheduleGroup",
        "scheduler:UntagResource"
      ],
      "Resource" : "arn:aws:scheduler:*:*:schedule-group/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "CreateSchedule",
      "Effect" : "Allow",
      "Action" : "scheduler:CreateScheduleGroup",
      "Resource" : "arn:aws:scheduler:*:*:schedule-group/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
```

```
          "aws:RequestTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "AmazonDataZone*"
        }
      }
    },
    {
      "Sid" : "TagSchedule",
      "Effect" : "Allow",
      "Action" : "scheduler:TagResource",
      "Resource" : "arn:aws:scheduler:*:*:schedule-group/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:TagKeys" : "false",
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "AmazonDataZone*"
        }
      }
    },
    {
      "Sid" : "DeleteSchedule",
      "Effect" : "Allow",
      "Action" : [
        "scheduler:DeleteSchedule"
      ],
      "Resource" : [
        "arn:aws:scheduler:*:*:schedule/SageMakerUnifiedStudio-*-*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
```

```
    {
      "Sid" : "ManageQSFolder",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:CreateDataSource",
        "quicksight:CreateFolder",
        "quicksight:CreateFolderMembership",
        "quicksight:CreateVPCConnection",
        "quicksight:DeleteDataSource",
        "quicksight:DeleteFolder",
        "quicksight:DescribeDataSource",
        "quicksight:DescribeFolderPermissions",
        "quicksight:DescribeDataSourcePermissions",
        "quicksight:DeleteVPCConnection",
        "quicksight:ListFolderMembers",
        "quicksight:ListTagsForResource",
        "quicksight:UpdateDataSource",
        "quicksight:UpdateDataSourcePermissions",
        "quicksight:UpdateFolder",
        "quicksight:UpdateFolderPermissions",
        "quicksight:UpdateVPCConnection"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "QuickSightResources",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeAccountSubscription",
        "quicksight:DescribeDataSet",
        "quicksight:DescribeDashboard",
        "quicksight:DescribeDashboardPermissions",
        "quicksight:DescribeFolder",
        "quicksight:DescribeGroup",
```

```
        "quicksight:DescribeGroupMembership",
        "quicksight:DescribeUser",
        "quicksight:DescribeVPCConnection",
        "quicksight:ListTagsForResource",
        "quicksight:UpdateDashboardPermissions"
      ],
      "Resource" : [
        "arn:aws:quicksight:*:*:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagQS",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:TagResource"
      ],
      "Resource" : [
        "arn:aws:quicksight:*:*:*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "PassRoleForQS",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSageMakerQuickSightVPC",
        "arn:aws:iam::*:role/datazone_usr_role_*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "quicksight.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PutRule",
      "Effect" : "Allow",
      "Action" : "events:PutRule",
      "Resource" : "arn:aws:events:*:*:rule/Managed.SageMaker*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "events:source" : [
            "aws.quicksight",
            "aws.codecommit"
          ]
        },
        "Null" : {
          "events:source" : "false",
          "events:detail-type" : "false"
        },
        "StringEquals" : {
          "events:ManagedBy" : "datazone.amazonaws.com",
          "events:detail-type" : [
            "AWS Service Event via CloudTrail",
            "CodeCommit Repository State Change"
          ],
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ManageEventRules",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DisableRule",
        "events:EnableRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/Managed.SageMaker*",
```

```
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "datazone.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RssAdmin",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "S3AGPerm",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetAccessGrantsInstance",
        "s3:CreateAccessGrantsInstance"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ResourceTagsUnTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:UntagResource",
        "neptune-graph:UntagResource",
        "quicksight:UntagResource",
```

```
        "glue:UntagResource",
        "airflow:UntagResource",
        "secretsmanager:UntagResource",
        "lambda:UntagResource",
        "emr-serverless:UntagResource",
        "elasticmapreduce:RemoveTags",
        "sagemaker:DeleteTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "SSOManage",
      "Effect" : "Allow",
      "Action" : [
        "sso:CreateApplication",
        "sso:DeleteApplication",
        "sso:DescribeApplication",
        "sso:DescribeInstance",
        "sso:ListInstances",
        "sso:PutApplicationAccessScope",
        "sso:PutApplicationAssignmentConfiguration",
        "sso:PutApplicationAuthenticationMethod",
        "sso:PutApplicationGrant",
        "sso:PutApplicationSessionConfiguration"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : [
            "elasticmapreduce.amazonaws.com",
            "emr-containers.amazonaws.com",
            "glue.amazonaws.com",
            "lakeformation.amazonaws.com",
            "ops.emr-serverless.amazonaws.com"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "EksClusterDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "eks:DescribeCluster"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EmrContainersManage",
      "Effect" : "Allow",
      "Action" : [
        "emr-containers:CreateManagedEndpoint",
        "emr-containers:CreateSecurityConfiguration",
        "emr-containers:CreateVirtualCluster",
        "emr-containers:DeleteManagedEndpoint",
        "emr-containers:DeleteSecurityConfiguration",
        "emr-containers:DeleteVirtualCluster",
        "emr-containers:DescribeSecurityConfiguration",
        "emr-containers:DescribeVirtualCluster",
        "emr-containers:DescribeManagedEndpoint",
        "emr-containers:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "ManageViaEmrContainers",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeNetworkInterfaces",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "eks:AssociateAccessPolicy",
```

```
        "eks:CreateAccessEntry",
        "eks:DisassociateAccessPolicy",
        "eks:DeleteAccessEntry",
        "eks:DescribeAccessEntry",
        "eks:ListAssociatedAccessPolicies"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : [
            "emr-containers.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

SageMakerStudioProjectRoleMachineLearningPolicy

説明: Amazon SageMaker Studio は、プロジェクトユーザーがデータ分析、人工知能、機械学習アクションを実行するための IAM ロールを作成し、これらのロールを作成して SageMaker に関連するアクセス許可を定義するときにこのポリシーを使用します。

`SageMakerStudioProjectRoleMachineLearningPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `SageMakerStudioProjectRoleMachineLearningPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 11 月 20 日 21:55 UTC
- 編集日時: 2025 年 11 月 21 日 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioProjectRoleMachineLearningPolicy`

ポリシーのバージョン

ポリシーのバージョン: v12 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowManageSageMakerEniOnVpc",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : [
            "sagemaker.amazonaws.com",
            "airflow.amazonaws.com"
          ]
        },
```

```
        "ArnLike" : {
          "ec2:Vpc" : "arn:aws:ec2:*:*:vpc/${aws:PrincipalTag/VpcId}"
        }
      }
    },
    {
      "Sid" : "AllowManageSageMakerTrainingEniOnVpc",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:AttachNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "ArnLike" : {
          "ec2:Vpc" : "arn:aws:ec2:*:*:vpc/${aws:PrincipalTag/VpcId}"
        }
      }
    },
    {
      "Sid" : "AllowManageSageMakerEni",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:AttachNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEqualsIfExists" : {
          "aws:CalledViaLast" : "sagemaker.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Sid" : "AllowSageMakerCreateVpcEndpointOnVpcId",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc/${aws:PrincipalTag/VpcId}",
      "Condition" : {
        "StringEquals" : {
          "ec2:VpcID" : "${aws:PrincipalTag/VpcId}"
        },
        "StringEqualsIfExists" : {
          "aws:CalledViaLast" : "sagemaker.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowSageMakerCreateVpcEndpoint",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEqualsIfExists" : {
          "aws:CalledViaLast" : "sagemaker.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowSageMakerDescribeVPCResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeSubnets",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "glue:ListSessions",
        "ec2:DescribeVpcs",
```

```
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeDhcpOptions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSageMakerLogAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:GetLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/sagemaker/*"
    },
    {
      "Sid" : "SageMakerMlflowPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:UpdateMlflowTrackingServer",
        "sagemaker:StartMlflowTrackingServer",
        "sagemaker:StopMlflowTrackingServer",
        "sagemaker:DescribeMlflowTrackingServer",
        "sagemaker:CreatePresignedMlflowTrackingServerUrl",
        "sagemaker-mlflow:*"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:mlflow-tracking-server/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SageMakerBYOFSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeMountTargets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerBYOIPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "sagemaker:DescribeImageVersion",
        "sagemaker:ListImageVersions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerStudioAppDescribeImageActionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeImage"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:image/*"
    },
    {
      "Sid" : "SageMakerPipelinesSTSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sts:GetCallerIdentity"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerLogPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/sagemaker/*"
    },
    {
      "Sid" : "SageMakerCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateTrainingJob",
        "sagemaker:CreateTransformJob",
        "sagemaker:CreateProcessingJob",
        "sagemaker:CreateAutoMLJob",
        "sagemaker:CreateAutoMLJobV2",
        "sagemaker:CreateHyperParameterTuningJob",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateEndpoint",
```

```
        "sagemaker:CreateModel",
        "sagemaker:CreateModelPackage",
        "sagemaker:CreateModelPackageGroup",
        "sagemaker:CreateInferenceComponent",
        "sagemaker:CreatePipeline",
        "sagemaker:CreateInferenceRecommendationsJob"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "SageMakerInferencePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:StopTrainingJob",
        "sagemaker:StopProcessingJob",
        "sagemaker:StopAutoMLJob",
        "sagemaker:StopHyperParameterTuningJob",
        "sagemaker:UpdateTrainingJob",
        "sagemaker:BatchGetMetrics",
        "sagemaker:BatchPutMetrics",
        "sagemaker:DeleteEndpointConfig",
        "sagemaker:DeleteEndpoint",
        "sagemaker:UpdateEndpoint",
        "sagemaker:UpdateEndpointWeightsAndCapacities",
        "sagemaker:UpdateInferenceComponentRuntimeConfig",
        "sagemaker:BatchDescribeModelPackage",
        "sagemaker:UpdateModelPackage",
        "sagemaker:DeleteModel",
        "sagemaker:DeleteModelPackage",
        "sagemaker:DeleteModelPackageGroup",
        "sagemaker:DeleteInferenceComponent",
        "sagemaker:InvokeEndpoint",
        "sagemaker:InvokeEndpointAsync",
        "sagemaker:InvokeEndpointWithResponseStream",
        "sagemaker:DescribeInferenceComponent",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeModel",
```

```
        "sagemaker:DescribeOptimizationJob",
        "sagemaker:DescribeEndpoint"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "SageMakerUpdateInferenceComponentRuntimeConfigAutoscalingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:UpdateInferenceComponentRuntimeConfig"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "application-autoscaling.amazonaws.com",
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "SageMakerDescribeUpdateDeletePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeInferenceRecommendationsJob",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:UpdatePipeline",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribePipelineExecution",
        "sagemaker:DescribePipelineDefinitionForExecution",
        "sagemaker:DeletePipeline",
        "sagemaker:UpdatePipelineExecution",
        "sagemaker:StartPipelineExecution",
        "sagemaker:StopPipelineExecution",
        "sagemaker:DescribeTransformJob",
        "sagemaker:StopTransformJob",
        "sagemaker:RetryPipelineExecution",
```

```
        "sagemaker:SendPipelineExecutionStepSuccess",
        "sagemaker:SendPipelineExecutionStepFailure",
        "sagemaker:DescribeHyperParameterTuningJob",
        "sagemaker:DescribeAutoMLJob",
        "sagemaker:DescribeAutoMLJobV2",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeTrainingJob"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "SageMakerLineageSpecialPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateContext",
        "sagemaker:CreateArtifact",
        "sagemaker:CreateAction",
        "sagemaker:AddAssociation",
        "sagemaker:DeleteAssociation",
        "sagemaker:DeleteContext",
        "sagemaker:DeleteAction",
        "sagemaker:DeleteArtifact"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "SageMakerModelRegistryLineageSpecialPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:QueryLineage",
```

```
        "sagemaker:DescribeAction",
        "sagemaker:DescribeArtifact",
        "sagemaker:DescribeTrialComponent",
        "sagemaker:DescribeContext"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:GetSearchSuggestions",
        "sagemaker:ListTrainingJobs",
        "sagemaker:ListTransformJobs",
        "sagemaker:ListProcessingJobs",
        "sagemaker:ListAutoMLJobs",
        "sagemaker:ListHyperParameterTuningJobs",
        "sagemaker:ListInferenceComponents",
        "sagemaker:ListEndpoints",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListModels",
        "sagemaker:ListModelPackages",
        "sagemaker:ListModelPackageGroups",
        "sagemaker:ListModelMetadata",
        "sagemaker:ListMlflowTrackingServers",
        "sagemaker:ListArtifacts",
        "sagemaker:ListHubs",
        "sagemaker:ListPipelines",
        "sagemaker:ListContexts"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "SageMakerSearchPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:Search"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true",
          "sagemaker:SearchVisibilityCondition/Tags.AmazonDataZoneProject/
EqualsIfExists" : "${aws:PrincipalTag/AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SageMakerListPermissionsTagRestricted",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListCandidatesForAutoMLJob",
        "sagemaker:ListTrainingJobsForHyperParameterTuningJob",
        "sagemaker:ListAssociations",
        "sagemaker:ListHubContents",
        "sagemaker:ListPipelineExecutionSteps",
        "sagemaker:ListPipelineExecutions",
        "sagemaker:ListPipelineParametersForExecution"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "SageMakerECRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchGetImage",
        "ecr:DescribeImages",
        "ecr:GetDownloadUrlForLayer"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/*"
    },
    {
      "Sid" : "SageMakerECRGetAuthorizationTokenPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryResourceGroupGetPermission",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:GetGroupQuery"
      ],
      "Resource" : "arn:aws:resource-groups:*:*:group/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryResourceGroupListPermission",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:ListGroupResources"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryResourceGroupWritePermission",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:Tag"
      ],
      "Resource" : "arn:aws:resource-groups:*:*:group/*",
      "Condition" : {
```

```
        "Null" : {
          "aws:ResourceTag/sagemaker:collection" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryResourceGroupDeletePermission",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:DeleteGroup"
      ],
      "Resource" : "arn:aws:resource-groups:*:*:group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:collection" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "SageMakerMLFlowModelRegistrationPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeModelPackageGroup"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:model-package-group/*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "SageMakerStudioCreatePresignedDomainUrlForUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreatePresignedDomainUrl"
```

```
      ],
      "Resource" : "arn:aws:sagemaker:*:*:user-profile/*/${aws:PrincipalTag/
datazone:userId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "SageMakerStudioCreatePresignedDomainUrlForTaggedUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreatePresignedDomainUrl"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:user-profile/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceTag/AmazonDataZoneUser" : "${aws:PrincipalTag/datazone:userId}",
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "SageMakerStudioAppListActionsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListApps",
        "sagemaker:ListDomains",
        "sagemaker:ListUserProfiles",
        "sagemaker:ListSpaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerStudioAppDescribeDomainActionsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeDomain"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SageMakerStudioAppDescribeJupyterLabAppActionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeApp"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:app/*/*/codeeditor/*",
        "arn:aws:sagemaker:*:*:app/*/*/CodeEditor/*",
        "arn:aws:sagemaker:*:*:app/*/*/jupyterlab/*",
        "arn:aws:sagemaker:*:*:app/*/*/JupyterLab/*"
      ]
    },
    {
      "Sid" : "SageMakerStudioAppDescribeUserProfileActionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeUserProfile"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:user-profile/*/${aws:PrincipalTag/
datazone:userId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SageMakerStudioAppDescribeTaggedUserProfilePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeUserProfile"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:user-profile/*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceTag/AmazonDataZoneUser" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "SMStudioAppDescribeSpaceActionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeSpace"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags",
        "sagemaker:DeleteTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        },
        "ForAllValues:StringNotLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "sagemaker:shared-with:*"
          ]
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "ProjectUserTag*",
            "sagemaker*",
            "sm-jumpstart*",
            "endpoint-has-jumpstart-model"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "SageMakerStudioAllowCreatingDeletingOwnerUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateUserProfile",
        "sagemaker:DeleteUserProfile"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:user-profile/*/${aws:PrincipalTag/
datazone:userId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SageMakerStudioAllowCreatingDeletingTaggedOwnerUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateUserProfile",
        "sagemaker:DeleteUserProfile"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:user-profile/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceTag/AmazonDataZoneUser" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "SageMakerStudioRestrictPrivateSpaceToOwnerUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateSpace",
        "sagemaker:UpdateSpace",
        "sagemaker:DeleteSpace"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:space/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "sagemaker:SpaceSharingType" : [
            "Private"
          ]
        },
        "ArnLike" : {
          "sagemaker:OwnerUserProfileArn" : "arn:aws:sagemaker:*:*:user-profile/*/
${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "SageMakerStudioRestrictPrivateSpaceToOwnerUser",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateSpace",
        "sagemaker:UpdateSpace",
        "sagemaker:DeleteSpace"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:space/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceTag/AmazonDataZoneUser" : "${aws:PrincipalTag/datazone:userId}",
          "sagemaker:SpaceSharingType" : [
            "Private"
          ]
        }
      }
    },
    {
      "Sid" : "SageMakerStudioRestrictPrivateSpaceAppsToOwnerUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateApp",
        "sagemaker:DeleteApp"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:app/*/*/codeeditor/*",
        "arn:aws:sagemaker:*:*:app/*/*/CodeEditor/*",
        "arn:aws:sagemaker:*:*:app/*/*/jupyterlab/*",
        "arn:aws:sagemaker:*:*:app/*/*/JupyterLab/*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "sagemaker:SpaceSharingType" : [
            "Private"
          ]
        },
        "ArnLike" : {
          "sagemaker:OwnerUserProfileArn" : "arn:aws:sagemaker:*:*:user-profile/*/
${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "SageMakerStudioRestrictPrivateSpaceAppsToOwnerUser",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateApp",
        "sagemaker:DeleteApp"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:app/*/*/CodeEditor/*",
        "arn:aws:sagemaker:*:*:app/*/*/codeeditor/*",
        "arn:aws:sagemaker:*:*:app/*/*/jupyterlab/*",
        "arn:aws:sagemaker:*:*:app/*/*/JupyterLab/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceTag/AmazonDataZoneUser" : "${aws:PrincipalTag/datazone:userId}",
          "sagemaker:SpaceSharingType" : [
            "Private"
          ]
        }
      }
    },
    {
      "Sid" : "AllowStartSessionForSpaceRemoteConnection",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:StartSession"
```

```
      ],
      "Resource" : "arn:aws:sagemaker:*:*:space/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceTag/AmazonDataZoneUser" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "PublishSagemakerMetric",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "cloudwatch:namespace" : "/aws/sagemaker/*"
        }
      }
    },
    {
      "Sid" : "ManageSageMakerEndpointsAutoscalingAlarms",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MutateSageMakerEndpointsAutoscalingAlarms",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:TargetTracking*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:CalledViaLast" : "application-autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SSMPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:GetParameters",
        "ssm:GetParametersByPath"
      ],
      "Resource" : "arn:aws:ssm:*::parameter/aws/service/sagemaker-distribution/*"
    },
    {
      "Sid" : "SageMakerJumpstartS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::jumpstart-cache-prod-*/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SageMakerCrossAccountPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:BatchDescribeModelPackage",
        "sagemaker:ListModelPackages",
        "sagemaker:CreateModel"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SageMakerListTagsRestrictionOnSharedResources",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListTags"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SageMakerAutoScalingPermissionsWithserviceNamespace",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:PutScheduledAction",
        "application-autoscaling:RegisterScalableTarget"
      ],
      "Resource" : "arn:aws:application-autoscaling:*:*:scalable-target/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "application-autoscaling:service-namespace" : "sagemaker"
        }
      }
    },
    {
      "Sid" : "SageMakerAutoScalingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
```

```
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions"
      ],
      "Resource" : "arn:aws:application-autoscaling:*:*:scalable-target/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SageMakerSLRForAutoScalingPermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "sagemaker.application-autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SageMakerKmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "sagemaker.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3AGObjectRead",
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetObjectAcl",
        "s3:GetObjectVersionAcl",
        "s3:ListMultipartUploadParts"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ArnEquals" : {
          "s3:AccessGrantsInstanceArn" : [
            "arn:aws:s3:*:*:access-grants/default"
          ]
        }
      }
    },
    {
      "Sid" : "S3AGObjectWrite",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:PutObjectVersionAcl",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:AbortMultipartUpload"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ArnEquals" : {
          "s3:AccessGrantsInstanceArn" : [
            "arn:aws:s3:*:*:access-grants/default"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "S3AGBucketLevelReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ArnEquals" : {
          "s3:AccessGrantsInstanceArn" : [
            "arn:aws:s3:*:*:access-grants/default"
          ]
        }
      }
    },
    {
      "Sid" : "S3AGKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:s3:arn"
        }
      }
    },
    {
      "Sid" : "S3AGLocationManagement",
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3:CreateAccessGrantsLocation",
        "s3:DeleteAccessGrantsLocation",
        "s3:GetAccessGrantsLocation"
      ],
      "Resource" : [
        "arn:aws:s3:*:*:access-grants/default/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "s3:accessGrantsLocationScope" : "s3://${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/"
        }
      }
    },
    {
      "Sid" : "S3AGPermissionManagement",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateAccessGrant",
        "s3:DeleteAccessGrant"
      ],
      "Resource" : [
        "arn:aws:s3:*:*:access-grants/default/location/*",
        "arn:aws:s3:*:*:access-grants/default/grant/*"
      ],
      "Condition" : {
        "StringLike" : {
          "s3:accessGrantScope" : "s3://${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/*"
        }
      }
    },
    {
      "Sid" : "CrossAccountS3AGResourceSharingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "ram:RequestedResourceType" : [
            "s3:AccessGrants"
          ]
```

```
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CrossAccountS3AGResourceSharingPolicyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutAccessGrantsInstanceResourcePolicy"
      ],
      "Resource" : "arn:aws:s3:*:*:access-grants/default",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3AGTaggingPermission",
      "Effect" : "Allow",
      "Action" : [
        "s3:TagResource",
        "s3:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:s3:*:*:access-grants/default/location/*",
        "arn:aws:s3:*:*:access-grants/default/grant/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ConsumerS3AGPermission",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetAccessGrantsInstanceForPrefix",
        "s3:GetDataAccess",
        "s3:ListCallerAccessGrants",
        "ram:GetResourceShareInvitations"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

SageMakerStudioProjectUserRolePermissionsBoundary

説明: Amazon SageMaker は、プロジェクトユーザーがデータ分析、人工知能、機械学習アクションを実行するための IAM ロールを作成し、それらのロールを作成してアクセス許可の範囲を定義するときにこのポリシーを使用します。

`SageMakerStudioProjectUserRolePermissionsBoundary` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `SageMakerStudioProjectUserRolePermissionsBoundary` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 11 月 20 日 21:57 UTC
- 編集日時: 2025 年 1 月 3 日 00:37 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioProjectUserRolePermissionsBoundary`

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DenyAllNonMatchingProjectTag",
      "Effect" : "Deny",
      "Action" : "*",
      "NotResource" : [
        "arn:*:sagemaker:*:*:model-package-group/*",
        "arn:*:sagemaker:*:*:model-package/*",
        "arn:*:glue:*:*:catalog/*",
        "arn:*:glue:*:*:database/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:PrincipalTag/AmazonDataZoneProject" : "false",
          "aws:PrincipalTag/SageMakerStudioQueryExecutionRole" : "true"
        },
        "StringNotEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "AmazonQChatPermissions",
      "Effect" : "Allow",
      "Action" : [
        "q:StartConversation",
        "q:SendMessage"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "DataLakeS3BucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SameAccountKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:ReEncryptFrom",
        "kms:ReEncryptTo",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "sqs.*.amazonaws.com",
            "sagemaker.*.amazonaws.com",
            "emr-serverless.*.amazonaws.com",
            "s3.*.amazonaws.com",
            "redshift.*.amazonaws.com",
            "redshift-serverless.*.amazonaws.com",
            "bedrock.*.amazonaws.com",
            "secretsmanager.*.amazonaws.com",
            "ec2.*.amazonaws.com",
            "codecommit.*.amazonaws.com",
            "glue.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "AllowGenerateDataKeyForEmrEbsEncryption",
      "Effect" : "Allow",
      "Action" : "kms:GenerateDataKey",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SameAccountKMSManagementPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListGrants",
        "kms:RevokeGrant",
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "sqs.*.amazonaws.com",
            "sagemaker.*.amazonaws.com",
            "emr-serverless.*.amazonaws.com",
            "s3.*.amazonaws.com",
            "redshift.*.amazonaws.com",
            "bedrock.*.amazonaws.com",
            "secretsmanager.*.amazonaws.com",
            "codecommit.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Sid" : "ListKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CrossAccountS3Permissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject*",
        "s3:PutObject",
        "s3:PutObjectRetention",
        "s3:RestoreObject",
        "s3:ReplicateObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:ListMultipartUploadParts",
        "s3:ListBucket",
        "s3:AbortMultipartUpload"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CrossAccountKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
```

```
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "s3.*.amazonaws.com",
            "sqs.*.amazonaws.com",
            "sagemaker.*.amazonaws.com"
          ]
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "CrossAccountKMSManagementPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListGrants",
        "kms:GetPublicKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "s3.*.amazonaws.com",
            "sqs.*.amazonaws.com",
            "sagemaker.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DataZoneKMSPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "datazone.*.amazonaws.com"
          ]
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "DataZoneDescribeKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "datazone.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ListDomainS3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListBucketVersions"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringLike" : {
```

```
          "s3:prefix" : [
            "${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/
AmazonDataZoneProject}",
            "${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/
AmazonDataZoneProject}/*"
          ]
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AirflowListDomainS3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : ""
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ListDomainBucketFromAthenaFederatedCatalog",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}"
      ],
      "Condition" : {
        "ArnEquals" : {
```

```
          "lambda:SourceFunctionArn" :
 "arn:aws:lambda:*:*:function:athenafederatedcatalog_*"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AccessDomainS3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject*",
        "s3:PutObject",
        "s3:PutObjectRetention",
        "s3:RestoreObject",
        "s3:ReplicateObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:ListMultipartUploadParts",
        "s3:AbortMultipartUpload"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AccessCertificateS3LocationPermissions",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/certificate_location/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
```

```
          "aws:PrincipalTag/AmazonDataZoneDomain" : ""
        },
        "Null" : {
          "aws:PrincipalTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagS3ObjectPermissionsForBedrockEvaluation",
      "Effect" : "Allow",
      "Action" : "s3:PutObjectTagging",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/
genAI/assets/evaluations/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        },
        "StringEquals" : {
          "s3:RequestObjectTag/BasicValidationStatus" : [
            "valid",
            "invalid"
          ],
          "s3:RequestObjectTag/ContainsReferenceResponseForAllPrompts" : [
            "true",
            "false"
          ]
        },
        "ForAllValues:StringEquals" : {
          "s3:RequestObjectTagKeys" : [
            "BasicValidationStatus",
            "ContainsReferenceResponseForAllPrompts"
          ]
        }
      }
    },
    {
      "Sid" : "CloudWatchDescribeLogGroups",
      "Effect" : "Allow",
```

```
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchLogsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:StartQuery",
        "logs:FilterLogEvents",
        "logs:GetLogEvents",
        "logs:GetLogRecord",
        "logs:GetLogGroupFields",
        "logs:GetQueryResults"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/*",
        "arn:aws:logs:*:*:log-group:airflow*",
        "arn:aws:logs:*:*:log-group:datazone*"
      ]
    },
    {
      "Sid" : "CloudWatchStopQuery",
      "Effect" : "Allow",
      "Action" : [
        "logs:StopQuery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AthenaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetTableMetadata",
        "athena:ListDatabases",
        "athena:ListDataCatalogs",
        "athena:ListEngineVersions",
```

```
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements",
        "athena:ListQueryExecutions",
        "athena:ListTableMetadata",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AthenaPermissionsWithResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "athena:TerminateSession",
        "athena:CreatePreparedStatement",
        "athena:StopCalculationExecution",
        "athena:StartQueryExecution",
        "athena:UpdatePreparedStatement",
        "athena:BatchGetNamedQuery",
        "athena:BatchGetPreparedStatement",
        "athena:BatchGetQueryExecution",
        "athena:UpdateNotebook",
        "athena:DeleteNotebook",
        "athena:DeletePreparedStatement",
        "athena:UpdateNotebookMetadata",
        "athena:DeleteNamedQuery",
        "athena:GetCalculationExecution",
        "athena:GetCalculationExecutionCode",
        "athena:GetCalculationExecutionStatus",
        "athena:GetNamedQuery",
        "athena:GetNotebookMetadata",
        "athena:GetPreparedStatement",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryResultsStream",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetSession",
        "athena:GetSessionStatus",
        "athena:GetWorkGroup",
        "athena:UpdateNamedQuery",
        "athena:CreateNamedQuery",
        "athena:ExportNotebook",
        "athena:StopQueryExecution",
        "athena:StartCalculationExecution",
```

```
        "athena:StartSession",
        "athena:CreatePresignedNotebookUrl",
        "athena:CreateNotebook",
        "athena:ImportNotebook",
        "athena:ListQueryExecutions",
        "athena:ListTagsForResource",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "DataZonePermissions",
      "Effect" : "Allow",
      "Action" : [
        "datazone:CreateConnection",
        "datazone:DeleteConnection",
        "datazone:GetConnection",
        "datazone:GetDomain",
        "datazone:GetDomainExecutionRoleCredentials",
        "datazone:GetEnvironment",
        "datazone:GetEnvironmentBlueprintConfiguration",
        "datazone:GetProject",
        "datazone:GetUserProfile",
        "datazone:ListConnections",
        "datazone:ListEnvironments",
        "datazone:ListEnvironmentBlueprints",
        "datazone:ListProjects",
        "datazone:UpdateConnection"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueDatalakePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateTable",
        "glue:DeleteTable",
        "glue:BatchDeleteTable",
```

```
        "glue:UpdateTable",
        "glue:BatchCreatePartition",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
        "glue:UpdatePartition",
        "glue:BatchGetPartition",
        "glue:BatchGetTableOptimizer",
        "glue:GetCatalogImportStatus",
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:GetColumnStatisticsTaskRun",
        "glue:GetColumnStatisticsTaskRuns",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetPartition",
        "glue:GetPartitionIndexes",
        "glue:GetPartitions",
        "glue:GetTable",
        "glue:GetTableOptimizer",
        "glue:GetTableVersion",
        "glue:GetTableVersions",
        "glue:GetTables",
        "glue:SearchTables",
        "glue:ListTableOptimizerRuns",
        "glue:CreatePartitionIndex",
        "glue:BatchUpdatePartition",
        "glue:DeleteTableVersion",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeletePartitionIndex",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:BatchDeleteTableVersion",
        "glue:GetCatalogs",
        "glue:GetCatalog",
        "glue:UpdateCatalog"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueCrawlerPermissions",
      "Effect" : "Allow",
      "Action" : "glue:ListCrawls",
```

```
      "Resource" : "arn:aws:glue:*:*:crawler/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueGlobalTempDatabasePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:DeleteDatabase",
        "glue:GetDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:database/global_temp",
        "arn:aws:glue:*:*:catalog"
      ]
    },
    {
      "Sid" : "GlueCatalogDatabasePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:DeleteDatabase",
        "glue:GetDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:catalog/*"
      ]
    },
    {
      "Sid" : "GlueUnrestrictedPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetClassifier",
        "glue:GetClassifiers",
        "glue:GetConnection",
        "glue:GetConnections",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:UseGlueStudio",
```

```
        "glue:ListSessions",
        "glue:StartCompletion",
        "glue:GetCompletion",
        "glue:GetGeneratedCode",
        "glue:GetTags"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GluePermissionsWithResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "glue:PassConnection",
        "glue:GetSession",
        "glue:GetStatement",
        "glue:CancelStatement",
        "glue:ListStatements",
        "glue:TagResource",
        "glue:UntagResource",
        "glue:DeleteSession",
        "glue:RunStatement",
        "glue:StopSession",
        "glue:GetDashboardUrl",
        "glue:NotifyEvent",
        "glue:StartBlueprintRun",
        "glue:PutWorkflowRunProperties",
        "glue:DeleteJob",
        "glue:DeleteWorkflow",
        "glue:DeleteBlueprint",
        "glue:UpdateWorkflow",
        "glue:UpdateJob",
        "glue:StartWorkflowRun",
        "glue:ResumeWorkflowRun",
        "glue:UpdateBlueprint",
        "glue:BatchStopJobRun",
        "glue:StopWorkflowRun",
        "glue:StartJobRun",
        "glue:CancelDataQualityRuleRecommendationRun",
        "glue:CancelDataQualityRulesetEvaluationRun",
        "glue:DeleteDataQualityRuleset",
        "glue:GetDataQualityModel",
        "glue:GetDataQualityModelResult",
        "glue:GetDataQualityResult",
        "glue:GetDataQualityRuleRecommendationRun",
```

```
        "glue:GetDataQualityRuleset",
        "glue:GetDataQualityRulesetEvaluationRun",
        "glue:ListDataQualityResults",
        "glue:ListDataQualityRuleRecommendationRuns",
        "glue:ListDataQualityRulesetEvaluationRuns",
        "glue:ListDataQualityRulesets",
        "glue:PublishDataQuality",
        "glue:PutDataQualityProfileAnnotation",
        "glue:PutDataQualityStatisticAnnotation",
        "glue:StartDataQualityRuleRecommendationRun",
        "glue:StartDataQualityRulesetEvaluationRun",
        "glue:UpdateDataQualityRuleset"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "GlueCreateAndTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateSession",
        "glue:CreateBlueprint",
        "glue:CreateJob",
        "glue:CreateDataQualityRuleset",
        "glue:CreateWorkflow",
        "glue:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "IAMListRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "IAMGetRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "IAMPassRolePermission",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com",
            "sagemaker.amazonaws.com",
            "ec2.amazonaws.com",
            "emr-serverless.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "RedshiftDataActionsIAMSessionRestriction",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:DescribeStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:CancelStatement",
        "redshift-data:ListStatements"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "redshift-data:statement-owner-iam-userid" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "RedshiftUnrestrictedPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "redshift:DescribeClusters",
        "sqlworkbench:PutTab",
        "sqlworkbench:DeleteTab",
        "sqlworkbench:DriverExecute",
        "sqlworkbench:GetUserInfo",
        "sqlworkbench:ListTabs",
        "sqlworkbench:GetAutocompletionMetadata",
        "sqlworkbench:GetAutocompletionResource",
        "sqlworkbench:PassAccountSettings",
        "sqlworkbench:ListQueryExecutionHistory",
        "sqlworkbench:GetQueryExecutionHistory",
        "sqlworkbench:CreateConnection",
        "sqlworkbench:PutQCustomContext",
        "sqlworkbench:GetQCustomContext",
        "sqlworkbench:DeleteQCustomContext",
        "sqlworkbench:GetQSqlRecommendations",
        "sqlworkbench:GetQSqlPromptQuotas",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftPermissionsWithResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:ListTagsForResource",
        "redshift:DescribeTags"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "AllowAccessExistingRedshiftCompute",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:GetCredentials",
        "redshift:DescribeTags",
        "redshift:GetClusterCredentialsWithIAM",
        "redshift-data:BatchExecuteStatement",
        "redshift-data:ExecuteStatement",
        "redshift-data:DescribeTable",
        "redshift-data:ListDatabases",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "RedshiftDataActionsForManagedWorkgroup",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:BatchExecuteStatement",
        "redshift-data:ExecuteStatement",
        "redshift-data:DescribeStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:CancelStatement",
        "redshift-data:GetStagingBucketLocation",
        "redshift-serverless:GetManagedWorkgroup"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringLike" : {
          "redshift-data:glue-catalog-arn" : "arn:aws:glue:*:*:catalog/*"
        }
      }
    },
    {
      "Sid" : "RedshifServerlessCredentialsForManagedWorkgroup",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetCredentials"
      ],
      "Resource" : "arn:aws:redshift-serverless:*:*:workgroup/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "redshift-data.amazonaws.com"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "RedshiftExistingComputeConnectToCatalog",
      "Effect" : "Allow",
      "Action" : [
        "redshift:GetClusterCredentialsWithIAM"
      ],
      "Resource" : "arn:aws:redshift:*:*:dbname:*/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "GenerativeAIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "codewhisperer:GenerateRecommendations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BedrockAppInferenceProfileInvocationPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetInferenceProfile",
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : "arn:aws:bedrock:*:*:application-inference-profile/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "BedrockModelInvocationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:*-model/*"
      ],
      "Condition" : {
        "Null" : {
          "bedrock:InferenceProfileArn" : "false"
        }
      }
    },
    {
      "Sid" : "ManageNetworkPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachNetworkInterface",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:CreateTags",
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeSubnets",
        "ec2:DescribeRouteTables",
```

```
        "ec2:DescribeSecurityGroups",
        "ec2:DeleteNetworkInterface",
        "ec2:DetachNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DeleteTags"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListImageVersions",
        "sagemaker:ListTrainingJobs",
        "sagemaker:ListTransformJobs",
        "sagemaker:ListProcessingJobs",
        "sagemaker:ListAutoMLJobs",
        "sagemaker:ListCandidatesForAutoMLJob",
        "sagemaker:ListContexts",
        "sagemaker:ListHyperParameterTuningJobs",
        "sagemaker:ListTrainingJobsForHyperParameterTuningJob",
        "sagemaker:ListInferenceComponents",
        "sagemaker:ListEndpoints",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListModels",
        "sagemaker:ListModelPackages",
        "sagemaker:ListModelPackageGroups",
        "sagemaker:ListModelMetadata",
        "sagemaker:ListMlflowTrackingServers",
        "sagemaker:ListArtifacts",
        "sagemaker:ListAssociations",
        "sagemaker:ListHubContents",
        "sagemaker:ListHubs",
        "sagemaker:ListPipelineExecutionSteps",
        "sagemaker:ListPipelineExecutions",
        "sagemaker:ListPipelineParametersForExecution",
        "sagemaker:ListPipelines",
        "sagemaker:ListApps",
        "sagemaker:ListDomains",
        "sagemaker:ListUserProfiles",
        "sagemaker:ListSpaces",
        "sagemaker:ListTags",
        "sagemaker:DescribeMlflowTrackingServer",
        "sagemaker:DescribeImageVersion",
```

```
        "sagemaker:DescribeImage",
        "sagemaker:DescribeInferenceComponent",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeOptimizationJob",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeInferenceRecommendationsJob",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribePipelineExecution",
        "sagemaker:DescribePipelineDefinitionForExecution",
        "sagemaker:DescribeHyperParameterTuningJob",
        "sagemaker:DescribeAutoMLJob",
        "sagemaker:DescribeAutoMLJobV2",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:DescribeAction",
        "sagemaker:DescribeArtifact",
        "sagemaker:DescribeTrialComponent",
        "sagemaker:DescribeContext",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeApp",
        "sagemaker:DescribeUserProfile",
        "sagemaker:DescribeSpace",
        "sagemaker:AddTags",
        "sagemaker:AddAssociation",
        "sagemaker:DeleteAssociation",
        "sagemaker:DeleteContext",
        "sagemaker:DeleteAction",
        "sagemaker:DeleteArtifact",
        "sagemaker:DeleteUserProfile",
        "sagemaker:UpdateSpace",
        "sagemaker:DeleteSpace",
        "sagemaker:DeleteApp",
        "sagemaker:CreatePresignedDomainUrl",
        "sagemaker:CreateUserProfile",
        "sagemaker:CreateSpace",
        "sagemaker:CreateApp",
        "sagemaker:CreateTrainingJob",
        "sagemaker:CreateTransformJob",
        "sagemaker:CreateProcessingJob",
        "sagemaker:CreateAutoMLJob",
        "sagemaker:CreateAutoMLJobV2",
```

```
        "sagemaker:CreateHyperParameterTuningJob",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateModel",
        "sagemaker:CreateModelPackage",
        "sagemaker:CreateModelPackageGroup",
        "sagemaker:CreatePipeline",
        "sagemaker:CreateContext",
        "sagemaker:CreateArtifact",
        "sagemaker:CreateAction",
        "sagemaker:CreateInferenceComponent",
        "sagemaker:UpdateInferenceComponentRuntimeConfig",
        "sagemaker:StopTrainingJob",
        "sagemaker:StopProcessingJob",
        "sagemaker:StopAutoMLJob",
        "sagemaker:StopHyperParameterTuningJob",
        "sagemaker:DescribeTransformJob",
        "sagemaker:StopTransformJob",
        "sagemaker:UpdateTrainingJob",
        "sagemaker:BatchGetMetrics",
        "sagemaker:BatchPutMetrics",
        "sagemaker:DeleteEndpointConfig",
        "sagemaker:DeleteEndpoint",
        "sagemaker:UpdateEndpoint",
        "sagemaker:UpdateEndpointWeightsAndCapacities",
        "sagemaker:BatchDescribeModelPackage",
        "sagemaker:UpdateModelPackage",
        "sagemaker:DeleteModel",
        "sagemaker:DeleteModelPackage",
        "sagemaker:DeleteModelPackageGroup",
        "sagemaker:DeleteTags",
        "sagemaker:DeleteInferenceComponent",
        "sagemaker:CreateInferenceRecommendationsJob",
        "sagemaker:InvokeEndpoint",
        "sagemaker:InvokeEndpointAsync",
        "sagemaker:InvokeEndpointWithResponseStream",
        "sagemaker:QueryLineage",
        "sagemaker:UpdatePipeline",
        "sagemaker:DeletePipeline",
        "sagemaker:UpdatePipelineExecution",
        "sagemaker:StartPipelineExecution",
        "sagemaker:StopPipelineExecution",
        "sagemaker:RetryPipelineExecution",
        "sagemaker:SendPipelineExecutionStepSuccess",
```

```
        "sagemaker:SendPipelineExecutionStepFailure",
        "sagemaker:GetSearchSuggestions",
        "sagemaker:Search",
        "sagemaker:UpdateMlflowTrackingServer",
        "sagemaker:StartMlflowTrackingServer",
        "sagemaker:StopMlflowTrackingServer",
        "sagemaker:CreatePresignedMlflowTrackingServerUrl",
        "sagemaker:ListPartnerApps",
        "sagemaker:CreatePartnerAppPresignedUrl",
        "sagemaker:DescribePartnerApp",
        "sagemaker:CallPartnerAppApi",
        "sagemaker-mlflow:AccessUI",
        "sagemaker-mlflow:CreateExperiment",
        "sagemaker-mlflow:SearchExperiments",
        "sagemaker-mlflow:GetExperiment",
        "sagemaker-mlflow:GetExperimentByName",
        "sagemaker-mlflow:DeleteExperiment",
        "sagemaker-mlflow:RestoreExperiment",
        "sagemaker-mlflow:UpdateExperiment",
        "sagemaker-mlflow:CreateRun",
        "sagemaker-mlflow:DeleteRun",
        "sagemaker-mlflow:RestoreRun",
        "sagemaker-mlflow:GetRun",
        "sagemaker-mlflow:LogMetric",
        "sagemaker-mlflow:LogBatch",
        "sagemaker-mlflow:LogModel",
        "sagemaker-mlflow:LogInputs",
        "sagemaker-mlflow:SetExperimentTag",
        "sagemaker-mlflow:SetTag",
        "sagemaker-mlflow:DeleteTag",
        "sagemaker-mlflow:LogParam",
        "sagemaker-mlflow:GetMetricHistory",
        "sagemaker-mlflow:SearchRuns",
        "sagemaker-mlflow:ListArtifacts",
        "sagemaker-mlflow:UpdateRun",
        "sagemaker-mlflow:CreateRegisteredModel",
        "sagemaker-mlflow:GetRegisteredModel",
        "sagemaker-mlflow:RenameRegisteredModel",
        "sagemaker-mlflow:UpdateRegisteredModel",
        "sagemaker-mlflow:DeleteRegisteredModel",
        "sagemaker-mlflow:GetLatestModelVersions",
        "sagemaker-mlflow:CreateModelVersion",
        "sagemaker-mlflow:GetModelVersion",
        "sagemaker-mlflow:UpdateModelVersion",
```

```
        "sagemaker-mlflow:DeleteModelVersion",
        "sagemaker-mlflow:SearchModelVersions",
        "sagemaker-mlflow:GetDownloadURIForModelVersionArtifacts",
        "sagemaker-mlflow:TransitionModelVersionStage",
        "sagemaker-mlflow:SearchRegisteredModels",
        "sagemaker-mlflow:SetRegisteredModelTag",
        "sagemaker-mlflow:DeleteRegisteredModelTag",
        "sagemaker-mlflow:DeleteModelVersionTag",
        "sagemaker-mlflow:DeleteRegisteredModelAlias",
        "sagemaker-mlflow:SetRegisteredModelAlias",
        "sagemaker-mlflow:GetModelVersionByAlias",
        "ecr:GetAuthorizationToken",
        "ecr:BatchGetImage",
        "ecr:GetDownloadUrlForLayer",
        "ecr:DescribeImages",
        "elasticfilesystem:DescribeMountTargets",
        "ssm:GetParameter",
        "ssm:GetParameters",
        "ssm:GetParametersByPath",
        "ec2:DescribeInstanceTypes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerSLRForAutoScalingPermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "sagemaker.application-autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ComputePermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:GetMetricData",
        "sts:GetCallerIdentity",
        "sts:TagSession",
```

```
        "emr-serverless:GetApplication",
        "emr-serverless:GetDashboardForJobRun",
        "emr-serverless:GetJobRun",
        "emr-serverless:ListApplications",
        "emr-serverless:ListJobRunAttempts",
        "emr-serverless:ListJobRuns",
        "emr-serverless:StartApplication",
        "emr-serverless:StartJobRun",
        "emr-serverless:StopApplication",
        "emr-serverless:AccessInteractiveEndpoints",
        "emr-serverless:AccessLivyEndpoints",
        "elasticmapreduce:ListReleaseLabels",
        "elasticmapreduce:ListSupportedInstanceTypes",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:CreatePersistentAppUI",
        "elasticmapreduce:DescribePersistentAppUI",
        "elasticmapreduce:GetPersistentAppUIPresignedURL",
        "pricing:GetProducts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAssumeAccessRole",
      "Effect" : "Allow",
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        }
      }
    },
    {
      "Sid" : "SetSourceIdentityForAssumeAccessRole",
      "Effect" : "Allow",
      "Action" : "sts:SetSourceIdentity",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "sts:SourceIdentity" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
```

```
    },
    {
      "Sid" : "AllowListSecrets",
      "Effect" : "Allow",
      "Action" : "secretsmanager:ListSecrets",
      "Resource" : "*"
    },
    {
      "Sid" : "ComputePermissionsWithResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:GetCredentials",
        "redshift-data:BatchExecuteStatement",
        "redshift-data:ExecuteStatement",
        "redshift-data:DescribeTable",
        "redshift-data:ListDatabases",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables",
        "elasticmapreduce:GetClusterSessionCredentials",
        "elasticmapreduce:GetManagedScalingPolicy",
        "elasticmapreduce:GetOnClusterAppUIPresignedURL",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListInstanceFleets",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListBootstrapActions",
        "elasticmapreduce:TerminateJobFlows",
        "redshift:GetClusterCredentialsWithIAM"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
```

```
    {
      "Sid" : "DataLakePermissions",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataAccess"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeCommitPermissions",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:BatchGetCommits",
        "codecommit:BatchGetPullRequests",
        "codecommit:BatchGetRepositories",
        "codecommit:BatchDescribeMergeConflicts",
        "codecommit:CreateBranch",
        "codecommit:CreateCommit",
        "codecommit:CreatePullRequest",
        "codecommit:DeleteBranch",
        "codecommit:DeleteFile",
        "codecommit:DescribeMergeConflicts",
        "codecommit:DescribePullRequestEvents",
        "codecommit:GetBlob",
        "codecommit:GetBranch",
        "codecommit:GetComment",
        "codecommit:GetCommentReactions",
        "codecommit:GetCommentsForComparedCommit",
        "codecommit:GetCommentsForPullRequest",
        "codecommit:GetCommit",
        "codecommit:GetCommitHistory",
        "codecommit:GetCommitsFromMergeBase",
        "codecommit:GetDifferences",
        "codecommit:GetFile",
        "codecommit:GetFolder",
        "codecommit:GetMergeCommit",
        "codecommit:GetMergeConflicts",
        "codecommit:GetMergeOptions",
        "codecommit:GetObjectIdentifier",
        "codecommit:GetPullRequest",
        "codecommit:GetPullRequestApprovalStates",
        "codecommit:GetPullRequestOverrideState",
        "codecommit:GetReferences",
        "codecommit:GetRepository",
```

```
        "codecommit:GetRepositoryTriggers",
        "codecommit:GetTree",
        "codecommit:GetUploadArchiveStatus",
        "codecommit:GitPull",
        "codecommit:GitPush",
        "codecommit:ListAssociatedApprovalRuleTemplatesForRepository",
        "codecommit:ListBranches",
        "codecommit:ListFileCommitHistory",
        "codecommit:ListPullRequests",
        "codecommit:ListTagsForResource",
        "codecommit:MergeBranchesByFastForward",
        "codecommit:MergeBranchesBySquash",
        "codecommit:MergeBranchesByThreeWay",
        "codecommit:MergePullRequestByFastForward",
        "codecommit:MergePullRequestBySquash",
        "codecommit:MergePullRequestByThreeWay",
        "codecommit:UpdateComment",
        "codecommit:UpdateDefaultBranch",
        "codecommit:UpdatePullRequestApprovalRuleContent",
        "codecommit:UpdatePullRequestApprovalState",
        "codecommit:UpdatePullRequestDescription",
        "codecommit:UpdatePullRequestStatus",
        "codecommit:UpdatePullRequestTitle",
        "codecommit:UpdateRepositoryDescription",
        "codecommit:PostCommentForComparedCommit",
        "codecommit:PostCommentForPullRequest",
        "codecommit:PostCommentReply",
        "codecommit:PutCommentReaction",
        "codecommit:PutFile"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "EMRServicePermissions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
```

```
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget",
        "application-autoscaling:DeleteScheduledAction",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScheduledActions",
        "application-autoscaling:PutScheduledAction",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "ec2:RunInstances",
        "ec2:CreateFleet",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion",
        "ec2:CreatePlacementGroup",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeletePlacementGroup",
        "ec2:ModifyInstanceAttribute",
        "ec2:TerminateInstances",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumeStatus",
        "ec2:DescribeVpcAttribute",
        "resource-groups:ListGroupResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ModelRegistryResourceGroupGetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:GetGroupQuery"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "ModelRegistryResourceGroupMutatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:DeleteGroup",
        "resource-groups:Tag"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:collection" : "false"
        }
      }
    },
    {
      "Sid" : "ModelRegistryBedRockPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:ListFoundationModels"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AccessAossCollectionsForBedrock",
      "Effect" : "Allow",
      "Action" : "aoss:APIAccessAll",
      "Resource" : "*"
    },
    {
      "Sid" : "AccessBedrockResources",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetAgent",
        "bedrock:GetAgentActionGroup",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:InvokeAgent",
        "bedrock:ListAgentActionGroups",
        "bedrock:ListAgentKnowledgeBases",
        "bedrock:Retrieve",
        "bedrock:StartIngestionJob",
        "bedrock:GetIngestionJob",
        "bedrock:ListIngestionJobs",
        "bedrock:ApplyGuardrail",
        "bedrock:ListPrompts",
```

```
        "bedrock:GetPrompt",
        "bedrock:CreatePrompt",
        "bedrock:DeletePrompt",
        "bedrock:CreatePromptVersion",
        "bedrock:InvokeFlow",
        "bedrock:GetEvaluationJob",
        "bedrock:CreateEvaluationJob",
        "bedrock:StopEvaluationJob",
        "bedrock:BatchDeleteEvaluationJob",
        "bedrock:ListTagsForResource",
        "bedrock:CreateAgentAlias",
        "bedrock:ListAgentAliases",
        "bedrock:GetAgentVersion",
        "bedrock:ListAgentVersions",
        "bedrock:DeleteAgentVersion",
        "bedrock:DeleteAgentAlias",
        "bedrock:GetAgentAlias",
        "bedrock:UpdateAgentAlias"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "CreateEvaluationJobForFoundationModel",
      "Effect" : "Allow",
      "Action" : "bedrock:CreateEvaluationJob",
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*",
        "arn:aws:bedrock:*:*:custom-model/*"
      ]
    },
    {
      "Sid" : "InvokeBedrockInlineAgentPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:InvokeInlineAgent",
      "Resource" : "*"
    },
    {
      "Sid" : "BedrockRetrieveAndGeneratePermissions",
```

```
      "Effect" : "Allow",
      "Action" : "bedrock:RetrieveAndGenerate",
      "Resource" : "*"
    },
    {
      "Sid" : "ListBedrockEvaluationJobPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:ListEvaluationJobs",
      "Resource" : "*"
    },
    {
      "Sid" : "PassRoleToBedrockEvaluation",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AmazonBedrockEvaluationRole-${aws:PrincipalTag/
AmazonDataZoneProject}-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "bedrock.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "TagBedrockResourcePermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:TagResource",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockKnowledgeBaseDataIngestionKmsPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/AmazonBedrockManaged" : "true"
        },
        "Null" : {
          "kms:ViaService" : "true",
          "kms:EncryptionContext:aws:bedrock:arn" : "false"
        }
      }
    },
    {
      "Sid" : "AccessSecretPermissionsForBedrockApp",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:amazon-bedrock-ide/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "InvokeFunctionPermissionsForBedrockApp",
      "Effect" : "Allow",
      "Action" : "lambda:InvokeFunction",
      "Resource" : "arn:aws:lambda:*:*:function:amazon-bedrock-ide-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "GetDataZoneEnvironmentCfnStackPermissionsForBedrockAppExport",
```

```
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:GetTemplate",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/DataZone-Env-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "MWAAPermissions",
      "Effect" : "Allow",
      "Action" : [
        "airflow:ListEnvironments",
        "airflow:GetEnvironment",
        "airflow:UpdateEnvironment",
        "airflow:CreateWebLoginToken",
        "airflow:InvokeRestApi"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AirflowS3GetAccountPublicAccessBlock",
      "Effect" : "Allow",
      "Action" : "s3:GetAccountPublicAccessBlock",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AirflowS3BucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetEncryptionConfiguration"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}"
    },
```

```
    {
      "Sid" : "SQSPermissionsForMWAA",
      "Effect" : "Allow",
      "Action" : [
        "sqs:ChangeMessageVisibility",
        "sqs:DeleteMessage",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ReceiveMessage",
        "sqs:SendMessage"
      ],
      "Resource" : "arn:aws:sqs:*:*:airflow-celery-*"
    },
    {
      "Sid" : "FederatedDataConnectionGlueSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "GlueConnectionAccessForFederatedDatabase",
      "Effect" : "Allow",
      "Action" : [
        "glue:ListConnectionTypes",
        "glue:DescribeConnectionType"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueEntitiesAccessForFederatedDatabase",
      "Effect" : "Allow",
      "Action" : [
        "glue:ListEntities",
        "glue:DescribeEntity",
```

```
        "glue:GetEntityRecords"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecretAccessForForUseWithAllDataZoneProjectsSecrets",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "AccessForDynamoDbConnections",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListTables"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "InvokeFunctionPermissionsForAthenaCatalogLambda",
      "Effect" : "Allow",
      "Action" : "lambda:InvokeFunction",
      "Resource" : "arn:aws:lambda:*:*:function:*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/SageMakerStudioQueryExecutionRole" : "true",
          "aws:ResourceTag/federated_athena_datacatalog" : "true"
        }
      }
    },
    {
      "Sid" : "ListDomainS3BucketForQueryExecutionRolePermissions",
      "Effect" : "Allow",
      "Action" : "s3:ListBucket",
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:PrincipalTag/SageMakerStudioQueryExecutionRole" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3PermissionsForAthenaCatalog",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource" : [
        "arn:aws:s3:::redshift-staging-bucket-*/*",
        "arn:aws:s3:::redshift-staging-bucket-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GetS3ObjectForQueryExecutionRolePermissions",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::*/dzd_*/*/dev/sys/athena/*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/SageMakerStudioQueryExecutionRole" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GetGlueUserDefinedFuncLakeFormationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetUserDefinedFunction",
        "glue:GetUserDefinedFunctions"
      ],
      "Resource" : [
```

```
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:database/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "glue:LakeFormationPermissions" : "Enabled"
        }
      }
    },
    {
      "Sid" : "GetGlueUserDefinedFuncPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetUserDefinedFunction",
        "glue:GetUserDefinedFunctions"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:userDefinedFunction/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "NotDeniedOperations",
      "Effect" : "Deny",
      "NotAction" : [
        "airflow:CreateWebLoginToken",
        "airflow:GetEnvironment",
        "airflow:InvokeRestApi",
        "airflow:ListEnvironments",
        "airflow:UpdateEnvironment",
        "aoss:APIAccessAll",
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeleteScheduledAction",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
```

```
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:PutScheduledAction",
        "application-autoscaling:RegisterScalableTarget",
        "athena:BatchGetNamedQuery",
        "athena:BatchGetPreparedStatement",
        "athena:BatchGetQueryExecution",
        "athena:CreateNamedQuery",
        "athena:CreateNotebook",
        "athena:CreatePreparedStatement",
        "athena:CreatePresignedNotebookUrl",
        "athena:DeleteNamedQuery",
        "athena:DeleteNotebook",
        "athena:DeletePreparedStatement",
        "athena:ExportNotebook",
        "athena:GetCalculationExecution",
        "athena:GetCalculationExecutionCode",
        "athena:GetCalculationExecutionStatus",
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetNamedQuery",
        "athena:GetNotebookMetadata",
        "athena:GetPreparedStatement",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryResultsStream",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetSession",
        "athena:GetSessionStatus",
        "athena:GetTableMetadata",
        "athena:GetWorkGroup",
        "athena:ImportNotebook",
        "athena:ListDatabases",
        "athena:ListDataCatalogs",
        "athena:ListEngineVersions",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements",
        "athena:ListQueryExecutions",
        "athena:ListTableMetadata",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups",
        "athena:StartCalculationExecution",
        "athena:StartQueryExecution",
        "athena:StartSession",
        "athena:StopCalculationExecution",
```

```
        "athena:StopQueryExecution",
        "athena:TerminateSession",
        "athena:UpdateNamedQuery",
        "athena:UpdateNotebook",
        "athena:UpdateNotebookMetadata",
        "athena:UpdatePreparedStatement",
        "bedrock:ApplyGuardrail",
        "bedrock:BatchDeleteEvaluationJob",
        "bedrock:CreateAgentAlias",
        "bedrock:CreateEvaluationJob",
        "bedrock:CreatePrompt",
        "bedrock:CreatePromptVersion",
        "bedrock:DeleteAgentAlias",
        "bedrock:DeleteAgentVersion",
        "bedrock:DeletePrompt",
        "bedrock:GetAgent",
        "bedrock:GetAgentActionGroup",
        "bedrock:GetAgentAlias",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:GetAgentVersion",
        "bedrock:GetEvaluationJob",
        "bedrock:GetInferenceProfile",
        "bedrock:GetIngestionJob",
        "bedrock:GetPrompt",
        "bedrock:InvokeAgent",
        "bedrock:InvokeFlow",
        "bedrock:InvokeInlineAgent",
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream",
        "bedrock:ListAgentActionGroups",
        "bedrock:ListAgentAliases",
        "bedrock:ListAgentKnowledgeBases",
        "bedrock:ListAgentVersions",
        "bedrock:ListEvaluationJobs",
        "bedrock:ListFoundationModels",
        "bedrock:ListIngestionJobs",
        "bedrock:ListPrompts",
        "bedrock:ListTagsForResource",
        "bedrock:Retrieve",
        "bedrock:RetrieveAndGenerate",
        "bedrock:StartIngestionJob",
        "bedrock:StopEvaluationJob",
        "bedrock:TagResource",
        "bedrock:UpdateAgentAlias",
```

```
        "cloudformation:DescribeStacks",
        "cloudformation:GetTemplate",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:PutMetricData",
        "codecommit:BatchDescribeMergeConflicts",
        "codecommit:BatchGetCommits",
        "codecommit:BatchGetPullRequests",
        "codecommit:BatchGetRepositories",
        "codecommit:CreateBranch",
        "codecommit:CreateCommit",
        "codecommit:CreatePullRequest",
        "codecommit:DeleteBranch",
        "codecommit:DeleteFile",
        "codecommit:DescribeMergeConflicts",
        "codecommit:DescribePullRequestEvents",
        "codecommit:GetBlob",
        "codecommit:GetBranch",
        "codecommit:GetComment",
        "codecommit:GetCommentReactions",
        "codecommit:GetCommentsForComparedCommit",
        "codecommit:GetCommentsForPullRequest",
        "codecommit:GetCommit",
        "codecommit:GetCommitHistory",
        "codecommit:GetCommitsFromMergeBase",
        "codecommit:GetDifferences",
        "codecommit:GetFile",
        "codecommit:GetFolder",
        "codecommit:GetMergeCommit",
        "codecommit:GetMergeConflicts",
        "codecommit:GetMergeOptions",
        "codecommit:GetObjectIdentifier",
        "codecommit:GetPullRequest",
        "codecommit:GetPullRequestApprovalStates",
        "codecommit:GetPullRequestOverrideState",
        "codecommit:GetReferences",
        "codecommit:GetRepository",
        "codecommit:GetRepositoryTriggers",
        "codecommit:GetTree",
        "codecommit:GetUploadArchiveStatus",
        "codecommit:GitPull",
```

```
        "codecommit:GitPush",
        "codecommit:ListAssociatedApprovalRuleTemplatesForRepository",
        "codecommit:ListBranches",
        "codecommit:ListFileCommitHistory",
        "codecommit:ListPullRequests",
        "codecommit:ListTagsForResource",
        "codecommit:MergeBranchesByFastForward",
        "codecommit:MergeBranchesBySquash",
        "codecommit:MergeBranchesByThreeWay",
        "codecommit:MergePullRequestByFastForward",
        "codecommit:MergePullRequestBySquash",
        "codecommit:MergePullRequestByThreeWay",
        "codecommit:PostCommentForComparedCommit",
        "codecommit:PostCommentForPullRequest",
        "codecommit:PostCommentReply",
        "codecommit:PutCommentReaction",
        "codecommit:PutFile",
        "codecommit:UpdateComment",
        "codecommit:UpdateDefaultBranch",
        "codecommit:UpdatePullRequestApprovalRuleContent",
        "codecommit:UpdatePullRequestApprovalState",
        "codecommit:UpdatePullRequestDescription",
        "codecommit:UpdatePullRequestStatus",
        "codecommit:UpdatePullRequestTitle",
        "codecommit:UpdateRepositoryDescription",
        "codewhisperer:GenerateRecommendations",
        "datazone:CreateConnection",
        "datazone:DeleteConnection",
        "datazone:GetConnection",
        "datazone:GetDomain",
        "datazone:GetDomainExecutionRoleCredentials",
        "datazone:GetEnvironment",
        "datazone:GetEnvironmentBlueprintConfiguration",
        "datazone:GetProject",
        "datazone:GetUserProfile",
        "datazone:ListConnections",
        "datazone:ListEnvironmentBlueprints",
        "datazone:ListEnvironments",
        "datazone:ListProjects",
        "datazone:UpdateConnection",
        "dynamodb:BatchGetItem",
        "dynamodb:BatchWriteItem",
        "dynamodb:Scan",
        "dynamodb:Query",
```

```
            "dynamodb:DescribeBackup",
            "dynamodb:DescribeContributorInsights",
            "dynamodb:DescribeContinuousBackups",
            "dynamodb:DescribeEndpoints",
            "dynamodb:DescribeExport",
            "dynamodb:DescribeGlobalTable",
            "dynamodb:DescribeGlobalTableSettings",
            "dynamodb:DescribeImport",
            "dynamodb:DescribeKinesisStreamingDestination",
            "dynamodb:DescribeLimits",
            "dynamodb:DescribeReservedCapacity",
            "dynamodb:DescribeReservedCapacityOfferings",
            "dynamodb:DescribeStream",
            "dynamodb:DescribeTable",
            "dynamodb:DescribeTableReplicaAutoScaling",
            "dynamodb:DescribeTimeToLive",
            "dynamodb:GetItem",
            "dynamodb:GetRecords",
            "dynamodb:ListExports",
            "dynamodb:ListGlobalTables",
            "dynamodb:ListImports",
            "dynamodb:ListTables",
            "dynamodb:ListTagsOfResource",
            "dynamodb:PutItem",
            "dynamodb:PartiQLSelect",
            "dynamodb:PartiQLInsert",
            "dynamodb:PartiQLUpdate",
            "dynamodb:PartiQLDelete",
            "dynamodb:UpdateItem",
            "dynamodb:UpdateGlobalTable",
            "dynamodb:UpdateTable",
            "ec2:AttachNetworkInterface",
            "ec2:AuthorizeSecurityGroupEgress",
            "ec2:AuthorizeSecurityGroupIngress",
            "ec2:CreateFleet",
            "ec2:CreateLaunchTemplate",
            "ec2:CreateLaunchTemplateVersion",
            "ec2:CreateNetworkInterface",
            "ec2:CreateNetworkInterfacePermission",
            "ec2:CreatePlacementGroup",
            "ec2:CreateSecurityGroup",
            "ec2:CreateTags",
            "ec2:CreateVpcEndpoint",
            "ec2:DeleteLaunchTemplate",
```

```
            "ec2:DeleteNetworkInterface",
            "ec2:DeleteNetworkInterfacePermission",
            "ec2:DeletePlacementGroup",
            "ec2:DeleteTags",
            "ec2:DescribeAccountAttributes",
            "ec2:DescribeCapacityReservations",
            "ec2:DescribeDhcpOptions",
            "ec2:DescribeImages",
            "ec2:DescribeInstances",
            "ec2:DescribeInstanceTypeOfferings",
            "ec2:DescribeInstanceTypes",
            "ec2:DescribeLaunchTemplates",
            "ec2:DescribeNetworkAcls",
            "ec2:DescribeNetworkInterfaces",
            "ec2:DescribePlacementGroups",
            "ec2:DescribeRouteTables",
            "ec2:DescribeSecurityGroups",
            "ec2:DescribeSubnets",
            "ec2:DescribeVolumes",
            "ec2:DescribeVolumeStatus",
            "ec2:DescribeVpcAttribute",
            "ec2:DescribeVpcEndpoints",
            "ec2:DescribeVpcs",
            "ec2:DetachNetworkInterface",
            "ec2:ModifyInstanceAttribute",
            "ec2:RevokeSecurityGroupEgress",
            "ec2:RevokeSecurityGroupIngress",
            "ec2:RunInstances",
            "ec2:TerminateInstances",
            "ecr:BatchGetImage",
            "ecr:DescribeImages",
            "ecr:GetAuthorizationToken",
            "ecr:GetDownloadUrlForLayer",
            "elasticfilesystem:DescribeMountTargets",
            "elasticmapreduce:CreatePersistentAppUI",
            "elasticmapreduce:DescribeCluster",
            "elasticmapreduce:DescribePersistentAppUI",
            "elasticmapreduce:GetClusterSessionCredentials",
            "elasticmapreduce:GetManagedScalingPolicy",
            "elasticmapreduce:GetOnClusterAppUIPresignedURL",
            "elasticmapreduce:GetPersistentAppUIPresignedURL",
            "elasticmapreduce:ListBootstrapActions",
            "elasticmapreduce:ListClusters",
            "elasticmapreduce:ListInstanceFleets",
```

```
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListReleaseLabels",
        "elasticmapreduce:ListSupportedInstanceTypes",
        "elasticmapreduce:TerminateJobFlows",
        "emr-serverless:AccessInteractiveEndpoints",
        "emr-serverless:AccessLivyEndpoints",
        "emr-serverless:GetApplication",
        "emr-serverless:GetDashboardForJobRun",
        "emr-serverless:GetJobRun",
        "emr-serverless:ListApplications",
        "emr-serverless:ListJobRunAttempts",
        "emr-serverless:ListJobRuns",
        "emr-serverless:StartApplication",
        "emr-serverless:StartJobRun",
        "emr-serverless:StopApplication",
        "glue:BatchCreatePartition",
        "glue:BatchDeletePartition",
        "glue:BatchDeleteTable",
        "glue:BatchDeleteTableVersion",
        "glue:BatchGetPartition",
        "glue:BatchGetTableOptimizer",
        "glue:BatchStopJobRun",
        "glue:BatchUpdatePartition",
        "glue:CancelDataQualityRuleRecommendationRun",
        "glue:CancelDataQualityRulesetEvaluationRun",
        "glue:CancelStatement",
        "glue:CreateBlueprint",
        "glue:CreateDatabase",
        "glue:CreateDataQualityRuleset",
        "glue:CreateJob",
        "glue:CreatePartition",
        "glue:CreatePartitionIndex",
        "glue:CreateSession",
        "glue:CreateTable",
        "glue:CreateWorkflow",
        "glue:DeleteBlueprint",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeleteDatabase",
        "glue:DeleteDataQualityRuleset",
        "glue:DeleteJob",
        "glue:DeletePartition",
        "glue:DeletePartitionIndex",
```

```
        "glue:DeleteSession",
        "glue:DeleteTable",
        "glue:DeleteTableVersion",
        "glue:DeleteWorkflow",
        "glue:DescribeConnectionType",
        "glue:DescribeEntity",
        "glue:GetCatalog",
        "glue:GetCatalogImportStatus",
        "glue:GetCatalogs",
        "glue:GetClassifier",
        "glue:GetClassifiers",
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:GetColumnStatisticsTaskRun",
        "glue:GetColumnStatisticsTaskRuns",
        "glue:GetCompletion",
        "glue:GetConnection",
        "glue:GetConnections",
        "glue:GetDashboardUrl",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetDataQualityModel",
        "glue:GetDataQualityModelResult",
        "glue:GetDataQualityResult",
        "glue:GetDataQualityRuleRecommendationRun",
        "glue:GetDataQualityRuleset",
        "glue:GetDataQualityRulesetEvaluationRun",
        "glue:GetEntityRecords",
        "glue:GetGeneratedCode",
        "glue:GetPartition",
        "glue:GetPartitionIndexes",
        "glue:GetPartitions",
        "glue:GetSession",
        "glue:GetStatement",
        "glue:GetTable",
        "glue:GetTableOptimizer",
        "glue:GetTables",
        "glue:GetTableVersion",
        "glue:GetTableVersions",
        "glue:GetTags",
        "glue:GetUserDefinedFunction",
        "glue:GetUserDefinedFunctions",
        "glue:ListConnectionTypes",
        "glue:ListCrawls",
```

```
        "glue:ListDataQualityResults",
        "glue:ListDataQualityRuleRecommendationRuns",
        "glue:ListDataQualityRulesetEvaluationRuns",
        "glue:ListDataQualityRulesets",
        "glue:ListEntities",
        "glue:ListSessions",
        "glue:ListStatements",
        "glue:ListTableOptimizerRuns",
        "glue:NotifyEvent",
        "glue:PassConnection",
        "glue:PublishDataQuality",
        "glue:PutDataQualityProfileAnnotation",
        "glue:PutDataQualityStatisticAnnotation",
        "glue:PutWorkflowRunProperties",
        "glue:ResumeWorkflowRun",
        "glue:RunStatement",
        "glue:SearchTables",
        "glue:StartBlueprintRun",
        "glue:StartCompletion",
        "glue:StartDataQualityRuleRecommendationRun",
        "glue:StartDataQualityRulesetEvaluationRun",
        "glue:StartJobRun",
        "glue:StartWorkflowRun",
        "glue:StopSession",
        "glue:StopWorkflowRun",
        "glue:TagResource",
        "glue:UntagResource",
        "glue:UpdateBlueprint",
        "glue:UpdateCatalog",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:UpdateDataQualityRuleset",
        "glue:UpdateJob",
        "glue:UpdatePartition",
        "glue:UpdateTable",
        "glue:UpdateWorkflow",
        "glue:UseGlueStudio",
        "iam:CreateServiceLinkedRole",
        "iam:GetRole",
        "iam:ListRoles",
        "iam:PassRole",
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:DescribeKey",
```

```
            "kms:Encrypt",
            "kms:GenerateDataKey",
            "kms:GenerateDataKeyWithoutPlaintext",
            "kms:GetPublicKey",
            "kms:ListAliases",
            "kms:ListGrants",
            "kms:ReEncryptFrom",
            "kms:ReEncryptTo",
            "kms:RevokeGrant",
            "lakeformation:GetDataAccess",
            "lambda:InvokeFunction",
            "logs:CreateLogGroup",
            "logs:CreateLogStream",
            "logs:DescribeLogGroups",
            "logs:DescribeLogStreams",
            "logs:FilterLogEvents",
            "logs:GetLogEvents",
            "logs:GetLogGroupFields",
            "logs:GetLogRecord",
            "logs:GetQueryResults",
            "logs:PutLogEvents",
            "logs:StartQuery",
            "logs:StopQuery",
            "pricing:GetProducts",
            "q:SendMessage",
            "q:StartConversation",
            "redshift-data:BatchExecuteStatement",
            "redshift-data:CancelStatement",
            "redshift-data:DescribeStatement",
            "redshift-data:DescribeTable",
            "redshift-data:ExecuteStatement",
            "redshift-data:GetStagingBucketLocation",
            "redshift-data:GetStatementResult",
            "redshift-data:ListDatabases",
            "redshift-data:ListSchemas",
            "redshift-data:ListStatements",
            "redshift-data:ListTables",
            "redshift-serverless:GetCredentials",
            "redshift-serverless:GetManagedWorkgroup",
            "redshift-serverless:GetNamespace",
            "redshift-serverless:GetWorkgroup",
            "redshift-serverless:ListNamespaces",
            "redshift-serverless:ListTagsForResource",
            "redshift-serverless:ListWorkgroups",
```

```
        "redshift:DescribeClusters",
        "redshift:DescribeTags",
        "redshift:GetClusterCredentialsWithIAM",
        "resource-groups:CreateGroup",
        "resource-groups:DeleteGroup",
        "resource-groups:GetGroupQuery",
        "resource-groups:ListGroupResources",
        "resource-groups:Tag",
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetBucketLocation",
        "s3:GetEncryptionConfiguration",
        "s3:GetObject*",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:ListMultipartUploadParts",
        "s3:PutObject",
        "s3:PutObjectRetention",
        "s3:PutObjectTagging",
        "s3:ReplicateObject",
        "s3:RestoreObject",
        "sagemaker-mlflow:AccessUI",
        "sagemaker-mlflow:CreateExperiment",
        "sagemaker-mlflow:CreateModelVersion",
        "sagemaker-mlflow:CreateRegisteredModel",
        "sagemaker-mlflow:CreateRun",
        "sagemaker-mlflow:DeleteExperiment",
        "sagemaker-mlflow:DeleteModelVersion",
        "sagemaker-mlflow:DeleteModelVersionTag",
        "sagemaker-mlflow:DeleteRegisteredModel",
        "sagemaker-mlflow:DeleteRegisteredModelAlias",
        "sagemaker-mlflow:DeleteRegisteredModelTag",
        "sagemaker-mlflow:DeleteRun",
        "sagemaker-mlflow:DeleteTag",
        "sagemaker-mlflow:GetDownloadURIForModelVersionArtifacts",
        "sagemaker-mlflow:GetExperiment",
        "sagemaker-mlflow:GetExperimentByName",
        "sagemaker-mlflow:GetLatestModelVersions",
        "sagemaker-mlflow:GetMetricHistory",
        "sagemaker-mlflow:GetModelVersion",
        "sagemaker-mlflow:GetModelVersionByAlias",
        "sagemaker-mlflow:GetRegisteredModel",
```

```
            "sagemaker-mlflow:GetRun",
            "sagemaker-mlflow:ListArtifacts",
            "sagemaker-mlflow:LogBatch",
            "sagemaker-mlflow:LogInputs",
            "sagemaker-mlflow:LogMetric",
            "sagemaker-mlflow:LogModel",
            "sagemaker-mlflow:LogParam",
            "sagemaker-mlflow:RenameRegisteredModel",
            "sagemaker-mlflow:RestoreExperiment",
            "sagemaker-mlflow:RestoreRun",
            "sagemaker-mlflow:SearchExperiments",
            "sagemaker-mlflow:SearchModelVersions",
            "sagemaker-mlflow:SearchRegisteredModels",
            "sagemaker-mlflow:SearchRuns",
            "sagemaker-mlflow:SetExperimentTag",
            "sagemaker-mlflow:SetRegisteredModelAlias",
            "sagemaker-mlflow:SetRegisteredModelTag",
            "sagemaker-mlflow:SetTag",
            "sagemaker-mlflow:TransitionModelVersionStage",
            "sagemaker-mlflow:UpdateExperiment",
            "sagemaker-mlflow:UpdateModelVersion",
            "sagemaker-mlflow:UpdateRegisteredModel",
            "sagemaker-mlflow:UpdateRun",
            "sagemaker:AddAssociation",
            "sagemaker:AddTags",
            "sagemaker:BatchDescribeModelPackage",
            "sagemaker:BatchGetMetrics",
            "sagemaker:BatchPutMetrics",
            "sagemaker:CallPartnerAppApi",
            "sagemaker:CreateAction",
            "sagemaker:CreateApp",
            "sagemaker:CreateArtifact",
            "sagemaker:CreateAutoMLJob",
            "sagemaker:CreateAutoMLJobV2",
            "sagemaker:CreateContext",
            "sagemaker:CreateEndpoint",
            "sagemaker:CreateEndpointConfig",
            "sagemaker:CreateHyperParameterTuningJob",
            "sagemaker:CreateInferenceComponent",
            "sagemaker:CreateInferenceRecommendationsJob",
            "sagemaker:CreateModel",
            "sagemaker:CreateModelPackage",
            "sagemaker:CreateModelPackageGroup",
            "sagemaker:CreatePartnerAppPresignedUrl",
```

```
        "sagemaker:CreatePipeline",
        "sagemaker:CreatePresignedDomainUrl",
        "sagemaker:CreatePresignedMlflowTrackingServerUrl",
        "sagemaker:CreateProcessingJob",
        "sagemaker:CreateSpace",
        "sagemaker:CreateTrainingJob",
        "sagemaker:CreateTransformJob",
        "sagemaker:CreateUserProfile",
        "sagemaker:DeleteAction",
        "sagemaker:DeleteApp",
        "sagemaker:DeleteArtifact",
        "sagemaker:DeleteAssociation",
        "sagemaker:DeleteContext",
        "sagemaker:DeleteEndpoint",
        "sagemaker:DeleteEndpointConfig",
        "sagemaker:DeleteInferenceComponent",
        "sagemaker:DeleteModel",
        "sagemaker:DeleteModelPackage",
        "sagemaker:DeleteModelPackageGroup",
        "sagemaker:DeletePipeline",
        "sagemaker:DeleteSpace",
        "sagemaker:DeleteTags",
        "sagemaker:DeleteUserProfile",
        "sagemaker:DescribeAction",
        "sagemaker:DescribeApp",
        "sagemaker:DescribeArtifact",
        "sagemaker:DescribeAutoMLJob",
        "sagemaker:DescribeAutoMLJobV2",
        "sagemaker:DescribeContext",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeHyperParameterTuningJob",
        "sagemaker:DescribeImage",
        "sagemaker:DescribeImageVersion",
        "sagemaker:DescribeInferenceComponent",
        "sagemaker:DescribeInferenceRecommendationsJob",
        "sagemaker:DescribeMlflowTrackingServer",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribeOptimizationJob",
        "sagemaker:DescribePartnerApp",
        "sagemaker:DescribePipeline",
```

```
        "sagemaker:DescribePipelineDefinitionForExecution",
        "sagemaker:DescribePipelineExecution",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeSpace",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:DescribeTransformJob",
        "sagemaker:DescribeTrialComponent",
        "sagemaker:DescribeUserProfile",
        "sagemaker:GetSearchSuggestions",
        "sagemaker:InvokeEndpoint",
        "sagemaker:InvokeEndpointAsync",
        "sagemaker:InvokeEndpointWithResponseStream",
        "sagemaker:ListApps",
        "sagemaker:ListArtifacts",
        "sagemaker:ListAssociations",
        "sagemaker:ListAutoMLJobs",
        "sagemaker:ListCandidatesForAutoMLJob",
        "sagemaker:ListContexts",
        "sagemaker:ListDomains",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListEndpoints",
        "sagemaker:ListHubContents",
        "sagemaker:ListHubs",
        "sagemaker:ListHyperParameterTuningJobs",
        "sagemaker:ListImageVersions",
        "sagemaker:ListInferenceComponents",
        "sagemaker:ListMlflowTrackingServers",
        "sagemaker:ListModelMetadata",
        "sagemaker:ListModelPackageGroups",
        "sagemaker:ListModelPackages",
        "sagemaker:ListModels",
        "sagemaker:ListPartnerApps",
        "sagemaker:ListPipelineExecutions",
        "sagemaker:ListPipelineExecutionSteps",
        "sagemaker:ListPipelineParametersForExecution",
        "sagemaker:ListPipelines",
        "sagemaker:ListProcessingJobs",
        "sagemaker:ListSpaces",
        "sagemaker:ListTags",
        "sagemaker:ListTrainingJobs",
        "sagemaker:ListTrainingJobsForHyperParameterTuningJob",
        "sagemaker:ListTransformJobs",
        "sagemaker:ListUserProfiles",
        "sagemaker:QueryLineage",
```

```
            "sagemaker:RetryPipelineExecution",
            "sagemaker:Search",
            "sagemaker:SendPipelineExecutionStepFailure",
            "sagemaker:SendPipelineExecutionStepSuccess",
            "sagemaker:StartMlflowTrackingServer",
            "sagemaker:StartPipelineExecution",
            "sagemaker:StopAutoMLJob",
            "sagemaker:StopHyperParameterTuningJob",
            "sagemaker:StopMlflowTrackingServer",
            "sagemaker:StopPipelineExecution",
            "sagemaker:StopProcessingJob",
            "sagemaker:StopTrainingJob",
            "sagemaker:StopTransformJob",
            "sagemaker:UpdateEndpoint",
            "sagemaker:UpdateEndpointWeightsAndCapacities",
            "sagemaker:UpdateInferenceComponentRuntimeConfig",
            "sagemaker:UpdateMlflowTrackingServer",
            "sagemaker:UpdateModelPackage",
            "sagemaker:UpdatePipeline",
            "sagemaker:UpdatePipelineExecution",
            "sagemaker:UpdateSpace",
            "sagemaker:UpdateTrainingJob",
            "secretsmanager:DescribeSecret",
            "secretsmanager:GetSecretValue",
            "secretsmanager:ListSecrets",
            "secretsmanager:PutSecretValue",
            "sqlworkbench:CreateConnection",
            "sqlworkbench:DeleteQCustomContext",
            "sqlworkbench:DeleteTab",
            "sqlworkbench:DriverExecute",
            "sqlworkbench:GetAutocompletionMetadata",
            "sqlworkbench:GetAutocompletionResource",
            "sqlworkbench:GetQCustomContext",
            "sqlworkbench:GetQSqlPromptQuotas",
            "sqlworkbench:GetQSqlRecommendations",
            "sqlworkbench:GetQueryExecutionHistory",
            "sqlworkbench:GetUserInfo",
            "sqlworkbench:ListQueryExecutionHistory",
            "sqlworkbench:ListTabs",
            "sqlworkbench:PassAccountSettings",
            "sqlworkbench:PutQCustomContext",
            "sqlworkbench:PutTab",
            "sqs:ChangeMessageVisibility",
            "sqs:DeleteMessage",
```

```
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ReceiveMessage",
        "sqs:SendMessage",
        "ssm:GetParameter",
        "ssm:GetParameters",
        "ssm:GetParametersByPath",
        "sts:AssumeRole",
        "sts:GetCallerIdentity",
        "sts:SetSourceIdentity",
        "sts:TagSession",
        "tag:GetResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

SageMakerStudioProjectUserRolePolicy

説明: Amazon SageMaker Studio は、プロジェクトユーザーがデータ分析、人工知能、機械学習アクションを実行するための IAM ロールを作成し、これらのロールを作成してアクセス許可を定義するときにこのポリシーを使用します。

`SageMakerStudioProjectUserRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `SageMakerStudioProjectUserRolePolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 11 月 20 日 21:59 UTC
- 編集日時: 2025 年 11 月 20 日 14:49 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioProjectUserRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v21 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CommonUserCodeCommitPermissions",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:BatchGetCommits",
        "codecommit:BatchGetPullRequests",
        "codecommit:BatchGetRepositories",
        "codecommit:BatchDescribeMergeConflicts",
        "codecommit:CreateBranch",
        "codecommit:CreateCommit",
        "codecommit:CreatePullRequest",
        "codecommit:DeleteBranch",
        "codecommit:DeleteFile",
        "codecommit:DescribeMergeConflicts",
        "codecommit:DescribePullRequestEvents",
        "codecommit:GetBlob",
        "codecommit:GetBranch",
        "codecommit:GetComment",
        "codecommit:GetCommentReactions",
        "codecommit:GetCommentsForComparedCommit",
```

```
        "codecommit:GetCommentsForPullRequest",
        "codecommit:GetCommit",
        "codecommit:GetCommitHistory",
        "codecommit:GetCommitsFromMergeBase",
        "codecommit:GetDifferences",
        "codecommit:GetFile",
        "codecommit:GetFolder",
        "codecommit:GetMergeCommit",
        "codecommit:GetMergeConflicts",
        "codecommit:GetMergeOptions",
        "codecommit:GetObjectIdentifier",
        "codecommit:GetPullRequest",
        "codecommit:GetPullRequestApprovalStates",
        "codecommit:GetPullRequestOverrideState",
        "codecommit:GetReferences",
        "codecommit:GetRepository",
        "codecommit:GetRepositoryTriggers",
        "codecommit:GetTree",
        "codecommit:GetUploadArchiveStatus",
        "codecommit:GitPull",
        "codecommit:GitPush",
        "codecommit:ListAssociatedApprovalRuleTemplatesForRepository",
        "codecommit:ListBranches",
        "codecommit:ListFileCommitHistory",
        "codecommit:ListPullRequests",
        "codecommit:ListTagsForResource",
        "codecommit:MergeBranchesByFastForward",
        "codecommit:MergeBranchesBySquash",
        "codecommit:MergeBranchesByThreeWay",
        "codecommit:MergePullRequestByFastForward",
        "codecommit:MergePullRequestBySquash",
        "codecommit:MergePullRequestByThreeWay",
        "codecommit:UpdateComment",
        "codecommit:UpdateDefaultBranch",
        "codecommit:UpdatePullRequestApprovalRuleContent",
        "codecommit:UpdatePullRequestApprovalState",
        "codecommit:UpdatePullRequestDescription",
        "codecommit:UpdatePullRequestStatus",
        "codecommit:UpdatePullRequestTitle",
        "codecommit:UpdateRepositoryDescription",
        "codecommit:PostCommentForComparedCommit",
        "codecommit:PostCommentForPullRequest",
        "codecommit:PostCommentReply",
        "codecommit:PutCommentReaction",
```

```
        "codecommit:PutFile"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "CodeCommitKmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:ReEncryptFrom",
        "kms:ReEncryptTo",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "codecommit.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContext:aws:codecommit:id" : "false"
        }
      }
    },
    {
      "Sid" : "AllowCodeWhispererGenerateRecommendations",
      "Effect" : "Allow",
      "Action" : [
        "codewhisperer:GenerateRecommendations"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "AllowGlueCreateEni",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "glue:RoleAssumedBy" : "glue.amazonaws.com"
        },
        "Null" : {
          "aws:TagKeys" : "true"
        }
      }
    },
    {
      "Sid" : "AllowGlueCreateEniOnSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "StringEquals" : {
          "glue:RoleAssumedBy" : "glue.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "AllowGlueCreateEniOnSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:subnet/*",
      "Condition" : {
        "StringEquals" : {
          "glue:RoleAssumedBy" : "glue.amazonaws.com"
        }
      }
```

```
    },
    {
      "Sid" : "AllowManageGlueEni",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface",
        "ec2:AttachNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "glue:RoleAssumedBy" : "glue.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/aws-glue-service-resource" : "false"
        }
      }
    },
    {
      "Sid" : "AllowAttachGlueEniOnInstance",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "glue:RoleAssumedBy" : "glue.amazonaws.com"
        },
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowDescribeGlueEni",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "glue:RoleAssumedBy" : "glue.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "FederatedDataConnectionGlueSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "glue:RoleAssumedBy" : "glue.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "GlueKernelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeSubnets",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "glue:ListSessions",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueCreateAndTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateSession",
        "glue:CreateBlueprint",
        "glue:CreateJob",
        "glue:CreateDataQualityRuleset",
        "glue:CreateWorkflow",
        "glue:TagResource"
```

```
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*",
        "arn:aws:glue:*:*:blueprint/*",
        "arn:aws:glue:*:*:job/*",
        "arn:aws:glue:*:*:dataQualityRuleset/*",
        "arn:aws:glue:*:*:workflow/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "ProjectUserTag*"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:PrincipalTag/EnableGlueWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "GlueTagSessionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:TagResource",
        "glue:UntagResource"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*",
        "arn:aws:glue:*:*:blueprint/*",
        "arn:aws:glue:*:*:job/*",
        "arn:aws:glue:*:*:dataQualityRuleset/*",
        "arn:aws:glue:*:*:workflow/*"
      ],
      "Condition" : {
        "ForAllValues:StringNotLike" : {
```

```
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "ProjectUserTag*"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:PrincipalTag/EnableGlueWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "GluePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CancelStatement",
        "glue:GetSession",
        "glue:ListStatements",
        "glue:DeleteSession",
        "glue:RunStatement",
        "glue:GetStatement",
        "glue:StopSession",
        "glue:GetDashboardUrl",
        "glue:NotifyEvent",
        "glue:StartBlueprintRun",
        "glue:PutWorkflowRunProperties",
        "glue:DeleteJob",
        "glue:DeleteWorkflow",
        "glue:DeleteBlueprint",
        "glue:UpdateWorkflow",
        "glue:UpdateJob",
        "glue:StartWorkflowRun",
        "glue:ResumeWorkflowRun",
        "glue:UpdateBlueprint",
        "glue:BatchStopJobRun",
        "glue:StopWorkflowRun",
        "glue:StartJobRun",
        "glue:CancelDataQualityRuleRecommendationRun",
```

```
        "glue:CancelDataQualityRulesetEvaluationRun",
        "glue:DeleteDataQualityRuleset",
        "glue:GetDataQualityModel",
        "glue:GetDataQualityModelResult",
        "glue:GetDataQualityResult",
        "glue:GetDataQualityRuleRecommendationRun",
        "glue:GetDataQualityRuleset",
        "glue:GetDataQualityRulesetEvaluationRun",
        "glue:ListDataQualityResults",
        "glue:ListDataQualityRuleRecommendationRuns",
        "glue:ListDataQualityRulesetEvaluationRuns",
        "glue:ListDataQualityRulesets",
        "glue:PublishDataQuality",
        "glue:PutDataQualityProfileAnnotation",
        "glue:PutDataQualityStatisticAnnotation",
        "glue:StartDataQualityRuleRecommendationRun",
        "glue:StartDataQualityRulesetEvaluationRun",
        "glue:UpdateDataQualityRuleset",
        "glue:GetJobRun",
        "glue:GetJobRuns",
        "glue:BatchGetJobs",
        "glue:GetJob"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*",
        "arn:aws:glue:*:*:blueprint/*",
        "arn:aws:glue:*:*:job/*",
        "arn:aws:glue:*:*:dataQualityRuleset/*",
        "arn:aws:glue:*:*:workflow/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:PrincipalTag/EnableGlueWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "GlueListJobsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:ListJobs"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:PrincipalTag/EnableGlueWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "GlueVisualETLPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetGeneratedCode"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueCompletionsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:StartCompletion",
        "glue:GetCompletion"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:completion/*",
        "arn:aws:glue:*:*:job/*"
      ]
    },
    {
      "Sid" : "GlueJobRunnerSessionLogPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws-glue/*"
    },
    {
      "Sid" : "EC2TagsPermissionsForGlue",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteTags",
```

```
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "aws-glue-*"
          ]
        },
        "StringEquals" : {
          "glue:RoleAssumedBy" : "glue.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueKmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : [
        "arn:aws:kms:*:*:key/${aws:PrincipalTag/DefaultGlueCatalogKmsKeyId}",
        "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}"
      ],
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "glue.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "kms:EncryptionContext:glue_catalog_id" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
```

```
      "Sid" : "EmrServerlessInteractivePermissions",
      "Effect" : "Allow",
      "Action" : [
        "emr-serverless:AccessInteractiveEndpoints",
        "emr-serverless:AccessLivyEndpoints",
        "emr-serverless:GetApplication",
        "emr-serverless:StartApplication",
        "emr-serverless:StopApplication"
      ],
      "Resource" : "arn:aws:emr-serverless:*:*:/applications/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "EmrServerlessJobAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "emr-serverless:GetDashboardForJobRun",
        "emr-serverless:GetJobRun"
      ],
      "Resource" : [
        "arn:aws:emr-serverless:*:*:/applications/*/jobruns/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "AirflowActionsForTaggedEnvironments",
      "Effect" : "Allow",
      "Action" : [
        "airflow:GetEnvironment",
        "airflow:UpdateEnvironment"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "AirflowListEnvironments",
      "Effect" : "Allow",
      "Action" : [
        "airflow:ListEnvironments"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AirflowUiApiAccess",
      "Effect" : "Allow",
      "Action" : [
        "airflow:CreateWebLoginToken",
        "airflow:InvokeRestApi"
      ],
      "Resource" : [
        "arn:aws:airflow:*:*:role/DataZoneMWAAEnv-${aws:PrincipalTag/
AmazonDataZoneDomain}-${aws:PrincipalTag/AmazonDataZoneProject}-${aws:PrincipalTag/
AmazonDataZoneScopeName}/User"
      ]
    },
    {
      "Sid" : "AirflowCloudwatchLogsActions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:PutLogEvents",
        "logs:GetLogEvents",
        "logs:GetLogRecord",
        "logs:GetLogGroupFields",
        "logs:GetQueryResults"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:airflow-DataZoneMWAAEnv-${aws:PrincipalTag/
AmazonDataZoneDomain}-${aws:PrincipalTag/AmazonDataZoneProject}-${aws:PrincipalTag/
AmazonDataZoneScopeName}-*"
      ]
    },
```

```
    {
      "Sid" : "AirflowCloudwatchActions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "cloudwatch:namespace" : "AmazonMWAA"
        }
      }
    },
    {
      "Sid" : "GlueJobCloudwatchPutMetricActions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "cloudwatch:namespace" : [
            "Glue",
            "AWS/Glue"
          ]
        }
      }
    },
    {
      "Sid" : "AirflowS3GetAccountPublicAccessBlock",
      "Effect" : "Allow",
      "Action" : "s3:GetAccountPublicAccessBlock",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AirflowSqsActions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "sqs:ChangeMessageVisibility",
        "sqs:DeleteMessage",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ReceiveMessage",
        "sqs:SendMessage"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:airflow-celery-*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AirflowS3BucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetEncryptionConfiguration",
        "s3:GetBucketPublicAccessBlock"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DataLakeS3BucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
```

```
      "Sid" : "DataLakeCrossAccountS3Permissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject*",
        "s3:ListMultipartUploadParts",
        "s3:ListBucket"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DataLakeCrossAccountKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListGrants",
        "kms:GetPublicKey",
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DataLakeCrossAccountDecryptKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
```

```
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:s3:arn"
        }
      }
    },
    {
      "Sid" : "ListDomainS3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListBucketVersions"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringLike" : {
          "s3:prefix" : [
            "${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/
AmazonDataZoneProject}",
            "${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/
AmazonDataZoneProject}/*"
          ]
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AirflowListDomainS3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : ""
```

```
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ListDomainBucketFromAthenaFederatedCatalog",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}"
      ],
      "Condition" : {
        "ArnEquals" : {
          "lambda:SourceFunctionArn" :
 "arn:aws:lambda:*:*:function:athenafederatedcatalog_*"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AccessDomainS3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject*",
        "s3:PutObject",
        "s3:PutObjectRetention",
        "s3:RestoreObject",
        "s3:ReplicateObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:ListMultipartUploadParts",
        "s3:AbortMultipartUpload"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
```

```
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AccessLevelControlS3BucketPermissions",
      "Effect" : "Allow",
      "Action" : "s3:GetBucketAcl",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagS3ObjectPermissionsForBedrockEvaluation",
      "Effect" : "Allow",
      "Action" : "s3:PutObjectTagging",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/
genAI/assets/evaluations/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        },
        "StringEquals" : {
          "s3:RequestObjectTag/BasicValidationStatus" : [
            "valid",
            "invalid"
          ],
          "s3:RequestObjectTag/ContainsReferenceResponseForAllPrompts" : [
            "true",
            "false"
          ]
        },
        "ForAllValues:StringEquals" : {
          "s3:RequestObjectTagKeys" : [
```

```
            "BasicValidationStatus",
            "ContainsReferenceResponseForAllPrompts"
          ]
        }
      }
    },
    {
      "Sid" : "AccessDomainS3BucketKmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : [
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/*"
          ]
        }
      }
    },
    {
      "Sid" : "DZDomainKMSKeyXAcctPerm",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/DomainKmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "kms:EncryptionContext:aws:datazone:domainId" : "${aws:PrincipalTag/
AmazonDataZoneDomain}",
          "kms:ViaService" : [
            "datazone.*.amazonaws.com"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "ListLogGroupsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueJobLogGroupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:StartQuery",
        "logs:GetLogEvents",
        "logs:GetLogRecord",
        "logs:GetLogGroupFields",
        "logs:GetQueryResults",
        "logs:PutLogEvents",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:FilterLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:${aws:PrincipalTag/LogGroupName}/output",
        "arn:aws:logs:*:*:log-group:${aws:PrincipalTag/LogGroupName}/error",
        "arn:aws:logs:*:*:log-group:${aws:PrincipalTag/LogGroupName}/output:log-
stream:*",
        "arn:aws:logs:*:*:log-group:${aws:PrincipalTag/LogGroupName}/error:log-
stream:*"
      ]
    },
    {
      "Sid" : "ProjectLogGroupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:StartQuery",
        "logs:GetLogEvents",
        "logs:GetLogRecord",
        "logs:GetLogGroupFields",
        "logs:GetQueryResults",
        "logs:PutLogEvents",
        "logs:CreateLogStream",
```

```
        "logs:FilterLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:${aws:PrincipalTag/LogGroupName}",
        "arn:aws:logs:*:*:log-group:${aws:PrincipalTag/LogGroupName}:log-stream:*"
      ]
    },
    {
      "Sid" : "CloudWatchStopQuery",
      "Effect" : "Allow",
      "Action" : [
        "logs:StopQuery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataLakeAthenaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "athena:TerminateSession",
        "athena:CreatePreparedStatement",
        "athena:StopCalculationExecution",
        "athena:StartQueryExecution",
        "athena:UpdatePreparedStatement",
        "athena:BatchGetNamedQuery",
        "athena:BatchGetPreparedStatement",
        "athena:BatchGetQueryExecution",
        "athena:UpdateNotebook",
        "athena:DeleteNotebook",
        "athena:DeletePreparedStatement",
        "athena:UpdateNotebookMetadata",
        "athena:DeleteNamedQuery",
        "athena:GetCalculationExecution",
        "athena:GetCalculationExecutionCode",
        "athena:GetCalculationExecutionStatus",
        "athena:GetNamedQuery",
        "athena:GetNotebookMetadata",
        "athena:GetPreparedStatement",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryResultsStream",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetSession",
        "athena:GetSessionStatus",
```

```
        "athena:GetWorkGroup",
        "athena:UpdateNamedQuery",
        "athena:CreateNamedQuery",
        "athena:ExportNotebook",
        "athena:StopQueryExecution",
        "athena:StartCalculationExecution",
        "athena:StartSession",
        "athena:CreatePresignedNotebookUrl",
        "athena:CreateNotebook",
        "athena:ImportNotebook",
        "athena:ListQueryExecutions",
        "athena:ListTagsForResource",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "DefaultAthenaDataCatalogPermissions",
      "Effect" : "Allow",
      "Action" : [
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetTableMetadata",
        "athena:ListDatabases",
        "athena:ListTableMetadata"
      ],
      "Resource" : [
        "arn:aws:athena:*:*:datacatalog/AwsDataCatalog",
        "arn:aws:athena:*:*:datacatalog/awsdatacatalog"
      ]
    },
    {
      "Sid" : "AthenaListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "athena:ListDataCatalogs",
        "athena:ListEngineVersions",
```

```
        "athena:ListWorkGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataZoneUserPermissions",
      "Effect" : "Allow",
      "Action" : [
        "datazone:CreateConnection",
        "datazone:DeleteConnection",
        "datazone:GetConnection",
        "datazone:GetDomain",
        "datazone:GetDomainExecutionRoleCredentials",
        "datazone:GetEnvironment",
        "datazone:GetEnvironmentBlueprintConfiguration",
        "datazone:GetProject",
        "datazone:GetUserProfile",
        "datazone:ListConnections",
        "datazone:ListEnvironments",
        "datazone:ListEnvironmentBlueprints",
        "datazone:ListProjects",
        "datazone:UpdateConnection",
        "datazone:PostLineageEvent"
      ],
      "Resource" : "arn:aws:datazone:*:*:domain/${aws:PrincipalTag/
AmazonDataZoneDomain}"
    },
    {
      "Sid" : "GlueGetDefaultDatabase",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/default"
      ]
    },
    {
      "Sid" : "AllowGlueGetDatabasesExceptDefault",
      "Effect" : "Allow",
      "Action" : "glue:GetDatabases",
      "NotResource" : "arn:aws:glue:*:*:database/default",
      "Condition" : {
```

```
        "StringEquals" : {
          "glue:LakeFormationPermissions" : "Enabled"
        }
      }
    },
    {
      "Sid" : "GlueListDatabasesOnNoDatabases",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabases"
      ],
      "Resource" : "arn:aws:glue:*:*:catalog"
    },
    {
      "Sid" : "GlueFileUploadPermissions",
      "Action" : [
        "glue:GetClassifier",
        "glue:GetClassifiers",
        "glue:UseGlueStudio"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    },
    {
      "Sid" : "GlueProjectConnectionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:PassConnection",
        "glue:GetConnection",
        "glue:GetConnections"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "GlueGetConnectionOnlyOnCatalog",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetConnection",
```

```
        "glue:GetConnections"
      ],
      "Resource" : "arn:aws:glue:*:*:catalog"
    },
    {
      "Sid" : "GlueDatalakePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateTable",
        "glue:DeleteTable",
        "glue:BatchDeleteTable",
        "glue:UpdateTable",
        "glue:BatchCreatePartition",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
        "glue:UpdatePartition",
        "glue:BatchGetPartition",
        "glue:BatchGetTableOptimizer",
        "glue:GetCatalogImportStatus",
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:GetColumnStatisticsTaskRun",
        "glue:GetColumnStatisticsTaskRuns",
        "glue:GetDatabase",
        "glue:DeleteDatabase",
        "glue:GetPartition",
        "glue:GetPartitionIndexes",
        "glue:GetPartitions",
        "glue:GetTable",
        "glue:GetTableOptimizer",
        "glue:GetTableVersion",
        "glue:GetTableVersions",
        "glue:GetTables",
        "glue:SearchTables",
        "glue:ListTableOptimizerRuns",
        "glue:CreatePartitionIndex",
        "glue:BatchUpdatePartition",
        "glue:DeleteTableVersion",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeletePartitionIndex",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
```

```
        "glue:BatchDeleteTableVersion",
        "glue:GetCatalogs",
        "glue:GetCatalog"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "glue:LakeFormationPermissions" : "Enabled"
        }
      }
    },
    {
      "Sid" : "GlueCrawlerPermissions",
      "Effect" : "Allow",
      "Action" : "glue:ListCrawls",
      "Resource" : "arn:aws:glue:*:*:crawler/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueGlobalTempDatabasePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:DeleteDatabase",
        "glue:GetDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:database/global_temp",
        "arn:aws:glue:*:*:catalog"
      ]
    },
    {
      "Sid" : "GlueDefaultCatalogsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetCatalog",
        "glue:UpdateCatalog"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "glue:LakeFormationPermissions" : "Enabled"
        }
      }
    },
    {
      "Sid" : "GlueNonDefaultCatalogsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetCatalog",
        "glue:UpdateCatalog"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "glue:LakeFormationPermissions" : "Enabled",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "GlueCatalogDatabasePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:DeleteDatabase",
        "glue:GetDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:catalog/*"
      ]
    },
    {
      "Sid" : "LakeFormationPermissionForDataLakeAccess",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataAccess",
        "lakeformation:GetResourceLFTags"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMListRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMGetRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowAssumeAccessRole",
      "Effect" : "Allow",
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        }
      }
    },
    {
      "Sid" : "SetSourceIdentityForAssumeAccessRole",
      "Effect" : "Allow",
      "Action" : "sts:SetSourceIdentity",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
```

```
          "sts:SourceIdentity" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "TagSessionForAssumeAccessRole",
      "Effect" : "Allow",
      "Action" : "sts:TagSession",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneProject",
            "AmazonDataZoneDomain"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:RequestTag/AmazonDataZoneDomain" : "${aws:PrincipalTag/
AmazonDataZoneDomain}"
        }
      }
    },
    {
      "Sid" : "SetContextForTrustedIdentityPropagation",
      "Effect" : "Allow",
      "Action" : [
        "sts:SetContext"
      ],
      "Resource" : [
        "arn:aws:sts::*:self"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "sqlworkbench.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "StsContext",
      "Effect" : "Allow",
```

```
      "Action" : "sts:SetContext",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:ArnEquals" : {
          "sts:RequestContextProviders" : [
            "arn:aws:iam::aws:contextProvider/IdentityCenter"
          ]
        },
        "Null" : {
          "sts:RequestContextProviders" : "false"
        }
      }
    },
    {
      "Sid" : "FederatedDataConnectionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetConnection",
        "glue:GetConnections",
        "glue:GetTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "UnRestrictedAccessForGlueEntities",
      "Effect" : "Allow",
      "Action" : [
        "glue:ListConnectionTypes",
        "glue:DescribeConnectionType"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueEntitiesAccessForFederatedDatabase",
      "Effect" : "Allow",
      "Action" : [
        "glue:ListEntities",
        "glue:DescribeEntity",
```

```
        "glue:GetEntityRecords"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowPassRoleOnProjectRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/${aws:PrincipalTag/RoleName}",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com",
            "glue.amazonaws.com",
            "airflow.amazonaws.com",
            "emr-serverless.amazonaws.com",
            "scheduler.amazonaws.com",
            "access-grants.s3.amazonaws.com"
          ],
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SQLWorkBenchActionsWithoutResourceType",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:PutTab",
        "sqlworkbench:DeleteTab",
        "sqlworkbench:DriverExecute",
        "sqlworkbench:GetUserInfo",
        "sqlworkbench:ListTabs",
        "sqlworkbench:GetAutocompletion*",
        "sqlworkbench:PassAccountSettings",
        "sqlworkbench:ListQueryExecutionHistory",
        "sqlworkbench:GetQueryExecutionHistory",
        "sqlworkbench:CreateConnection",
        "sqlworkbench:*QCustomContext",
        "sqlworkbench:GetQSql*",
        "sqlworkbench:GetSchemaInference"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "SQLWorkBenchActions",
      "Effect" : "Allow",
      "Action" : "sqlworkbench:AssociateNotebookWithTab",
      "Resource" : "arn:*:sqlworkbench:*:*:notebook/*"
    },
    {
      "Sid" : "SQLWorkBenchNotebookActions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:CreateNotebook*",
        "sqlworkbench:GetNotebook",
        "sqlworkbench:UpdateNotebook*",
        "sqlworkbench:DeleteNotebook*",
        "sqlworkbench:ExportNotebook",
        "sqlworkbench:BatchGetNotebookCell",
        "sqlworkbench:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "RedshiftDataActionsIAMSessionRestriction",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:DescribeStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:CancelStatement",
        "redshift-data:ListStatements"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "redshift-data:statement-owner-iam-userid" : "${aws:userid}"
        }
      }
    },
```

```
    {
      "Sid" : "RedshiftDataActionsForResources",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:BatchExecuteStatement",
        "redshift-data:ExecuteStatement",
        "redshift-data:DescribeTable",
        "redshift-data:ListDatabases",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "AllowAccessExistingRedshiftCompute",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:GetCredentials",
        "redshift:DescribeTags",
        "redshift:GetClusterCredentialsWithIAM",
        "redshift-data:BatchExecuteStatement",
        "redshift-data:ExecuteStatement",
        "redshift-data:DescribeTable",
        "redshift-data:ListDatabases",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "true"
        }
```

```
      }
    },
    {
      "Sid" : "RedshiftWithoutResourceType",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "redshift:DescribeClusters"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftServerlessWorkgroupWithResourceType",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:GetNamespace",
        "redshift:DescribeTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "RedshiftExistingComputeConnectToCatalog",
      "Effect" : "Allow",
      "Action" : [
        "redshift:GetClusterCredentialsWithIAM"
      ],
      "Resource" : "arn:aws:redshift:*:*:dbname:*/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "AllowListSecrets",
```

```
      "Effect" : "Allow",
      "Action" : "secretsmanager:ListSecrets",
      "Resource" : "*"
    },
    {
      "Sid" : "ComputeCredentials",
      "Effect" : "Allow",
      "Action" : [
        "emr-containers:DescribeManagedEndpoint",
        "emr-containers:DescribeSecurityConfiguration",
        "emr-containers:DescribeVirtualCluster",
        "emr-containers:GetManagedEndpointSessionCredentials",
        "redshift-serverless:GetCredentials",
        "redshift:GetClusterCredentialsWithIAM"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "RedshiftDataActionsForManagedWorkgroup",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:BatchExecuteStatement",
        "redshift-data:ExecuteStatement",
        "redshift-data:DescribeStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:CancelStatement",
        "redshift-data:GetStagingBucketLocation",
        "redshift-serverless:GetManagedWorkgroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "redshift-data:glue-catalog-arn" : "arn:aws:glue:*:*:catalog/*"
        }
      }
    },
    {
      "Sid" : "RedshifServerlessCredentialsForManagedWorkgroup",
```

```
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetCredentials"
      ],
      "Resource" : "arn:aws:redshift-serverless:*:*:workgroup/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "redshift-data.amazonaws.com",
            "sqlworkbench.amazonaws.com"
          ]
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "AllowTagGetResources",
      "Effect" : "Allow",
      "Action" : "tag:GetResources",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "sqlworkbench.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowGetSecretForRedShift",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
```

```
      "Sid" : "CloudWatchMetricsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonQChatPermissions",
      "Effect" : "Allow",
      "Action" : [
        "q:StartConversation",
        "q:SendMessage"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EMRClusterWithDataZoneTags",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListInstanceFleets",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListBootstrapActions",
        "elasticmapreduce:GetManagedScalingPolicy",
        "elasticmapreduce:GetOnClusterAppUIPresignedURL"
      ],
      "Resource" : [
        "arn:aws:elasticmapreduce:*:*:cluster/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "EMRClusterInfoPermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:ListReleaseLabels",
```

```
        "elasticmapreduce:ListSupportedInstanceTypes",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:CreatePersistentAppUI",
        "elasticmapreduce:DescribePersistentAppUI",
        "pricing:GetProducts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EMRGetClusterSessionCredentials",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:GetClusterSessionCredentials"
      ],
      "Resource" : [
        "arn:aws:elasticmapreduce:*:*:cluster/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        },
        "ArnLike" : {
          "elasticmapreduce:ExecutionRoleArn" : "arn:aws:iam::*:role/
${aws:PrincipalTag/RoleName}"
        }
      }
    },
    {
      "Sid" : "EmrContainersSSO",
      "Effect" : "Allow",
      "Action" : [
        "sso:DescribeApplication"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : [
            "emr-containers.amazonaws.com"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "EMRPersistentAppUI",
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "elasticmapreduce:GetPersistentAppUIPresignedURL"
      ],
      "Condition" : {
        "ArnLike" : {
          "elasticmapreduce:ExecutionRoleArn" : "arn:aws:iam::*:role/
${aws:PrincipalTag/RoleName}"
        }
      }
    },
    {
      "Sid" : "KmsWithEncrypt",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:ReEncryptFrom",
        "kms:ReEncryptTo",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "sqs.*.amazonaws.com",
            "sagemaker.*.amazonaws.com",
            "bedrock.*.amazonaws.com",
            "s3.*.amazonaws.com",
            "scheduler.*.amazonaws.com",
            "glue.*.amazonaws.com",
            "secretsmanager.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
```

```
      }
    },
    {
      "Sid" : "EBDecrypt",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:scheduler:schedule:arn" : "false"
        }
      }
    },
    {
      "Sid" : "KmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:ReEncryptFrom",
        "kms:ReEncryptTo",
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "emr-serverless.*.amazonaws.com",
            "redshift.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "KmsManagement",
```

```
      "Effect" : "Allow",
      "Action" : [
        "kms:ListGrants",
        "kms:RevokeGrant",
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "sqs.*.amazonaws.com",
            "sagemaker.*.amazonaws.com",
            "emr-serverless.*.amazonaws.com",
            "s3.*.amazonaws.com",
            "redshift.*.amazonaws.com",
            "codecommit.*.amazonaws.com",
            "scheduler.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AwsOwnedKmsKeyPermissions",
      "Action" : [
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:kms:*:*:key/*"
      ],
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "s3.*.amazonaws.com",
            "sqs.*.amazonaws.com",
            "sagemaker.*.amazonaws.com"
          ]
```

```
        },
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "AwsOwnedKmsManagement",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:kms:*:*:key/*"
      ],
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "sqs.*.amazonaws.com",
            "sagemaker.*.amazonaws.com"
          ]
        },
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ListKMS",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
```

```
      "Sid" : "EC2PermissionsForNotebookExecution",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceTypes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "InvokeBedrockModel",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*",
        "arn:aws:bedrock:*:*:custom-model/*",
        "arn:aws:bedrock:*:*:provisioned-model/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true"
        },
        "Null" : {
          "bedrock:InferenceProfileArn" : "false"
        }
      }
    },
    {
      "Sid" : "BedrockInvokeModelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*",
        "arn:aws:bedrock:*:*:custom-model/*",
        "arn:aws:bedrock:*:*:provisioned-model/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true"
        },
```

```
        "ArnLike" : {
          "bedrock:InferenceProfileArn" : "arn:aws:bedrock:*:*:application-inference-
profile/*"
        }
      }
    },
    {
      "Sid" : "InvokeBedrockModelAppInferenceProfilePermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetInferenceProfile",
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : "arn:aws:bedrock:*:*:application-inference-profile/*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockInvokeModelAppInferenceProfilePermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetInferenceProfile",
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : "arn:aws:bedrock:*:*:application-inference-profile/*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "AccessBedrockResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "bedrock:InvokeAgent",
        "bedrock:Retrieve",
        "bedrock:ListIngestionJobs",
        "bedrock:StartIngestionJob",
        "bedrock:GetIngestionJob",
        "bedrock:ApplyGuardrail",
        "bedrock:ListPrompts",
        "bedrock:GetPrompt",
        "bedrock:CreatePrompt",
        "bedrock:DeletePrompt",
        "bedrock:CreatePromptVersion",
        "bedrock:InvokeFlow",
        "bedrock:GetEvaluationJob",
        "bedrock:CreateEvaluationJob",
        "bedrock:StopEvaluationJob",
        "bedrock:BatchDeleteEvaluationJob",
        "bedrock:ListTagsForResource",
        "bedrock:CreateAgentAlias",
        "bedrock:ListAgentAliases",
        "bedrock:GetAgentVersion",
        "bedrock:ListAgentVersions",
        "bedrock:DeleteAgentVersion",
        "bedrock:DeleteAgentAlias",
        "bedrock:GetAgentAlias",
        "bedrock:UpdateAgentAlias"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockResourceAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:ApplyGuardrail",
        "bedrock:BatchDeleteEvaluationJob",
        "bedrock:CreateAgentAlias",
        "bedrock:CreateBlueprint",
        "bedrock:CreateBlueprintVersion",
```

```
        "bedrock:CreateDataAutomationProject",
        "bedrock:CreateEvaluationJob",
        "bedrock:CreatePrompt",
        "bedrock:CreatePromptVersion",
        "bedrock:DeleteAgentAlias",
        "bedrock:DeleteAgentVersion",
        "bedrock:DeleteBlueprint",
        "bedrock:DeleteDataAutomationProject",
        "bedrock:DeletePrompt",
        "bedrock:GetAgentAlias",
        "bedrock:GetAgentVersion",
        "bedrock:GetBlueprint",
        "bedrock:GetDataAutomationProject",
        "bedrock:GetDataAutomationStatus",
        "bedrock:GetEvaluationJob",
        "bedrock:GetIngestionJob",
        "bedrock:GetPrompt",
        "bedrock:InvokeAgent",
        "bedrock:InvokeDataAutomationAsync",
        "bedrock:InvokeFlow",
        "bedrock:ListAgentAliases",
        "bedrock:ListAgentVersions",
        "bedrock:ListIngestionJobs",
        "bedrock:ListPrompts",
        "bedrock:ListTagsForResource",
        "bedrock:Retrieve",
        "bedrock:StartIngestionJob",
        "bedrock:StopEvaluationJob",
        "bedrock:UpdateAgentAlias",
        "bedrock:UpdateBlueprint",
        "bedrock:UpdateDataAutomationProject",
        "bedrock:ListAgentActionGroups",
        "bedrock:ListAgentKnowledgeBases"
      ],
      "Resource" : "arn:aws:bedrock:*:*:*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
```

```
      "Sid" : "CreateEvaluationJobForFoundationModelPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:CreateEvaluationJob",
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*",
        "arn:aws:bedrock:*:*:custom-model/*"
      ]
    },
    {
      "Sid" : "BedrockCreateEvaluationJobPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:CreateEvaluationJob",
      "Resource" : [
        "arn:aws:bedrock:*:*:custom-model/*",
        "arn:aws:bedrock:*::foundation-model/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "InvokeDataAutomationAsyncPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeDataAutomationAsync"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:data-automation-profile/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "InvokeBedrockInlineAgentPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:InvokeInlineAgent",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true",
          "bedrock:InlineAgentName" : "${datazone:userId}"
        },
        "StringNotEquals" : {
          "bedrock:InlineAgentName" : ""
        }
      }
    },
    {
      "Sid" : "BedrockInvokeInlineAgentPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:InvokeInlineAgent",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true",
          "bedrock:InlineAgentName" : "${datazone:userId}"
        },
        "StringNotEquals" : {
          "bedrock:InlineAgentName" : ""
        }
      }
    },
    {
      "Sid" : "BedrockRetrieveAndGeneratePermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:RetrieveAndGenerate",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "ListBedrockEvaluationJobPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:ListEvaluationJobs",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true"
        }
      }
```

```
    },
    {
      "Sid" : "BedrockNoResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:ListEvaluationJobs",
        "bedrock:RetrieveAndGenerate",
        "bedrock:ListFoundationModels"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "PassRoleToBedrockEvaluation",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AmazonBedrockEvaluationRole-${aws:PrincipalTag/
AmazonDataZoneProject}-*",
        "arn:aws:iam::*:role/AmazonBedrockServiceRole-${aws:PrincipalTag/
AmazonDataZoneProject}-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true",
          "iam:PassedToService" : [
            "bedrock.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "IamPassRoleToBedrockPermissions",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/AmazonBedrockEvaluationRole-${aws:PrincipalTag/
AmazonDataZoneProject}-*",
```

```
        "arn:aws:iam::*:role/AmazonBedrockServiceRole-${aws:PrincipalTag/
AmazonDataZoneProject}-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true",
          "iam:PassedToService" : "bedrock.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "TagBedrockResourcePermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:TagResource",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true",
          "aws:RequestTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "AmazonBedrockManaged",
            "ProjectUserTag*"
          ]
        }
      }
    },
    {
      "Sid" : "BedrockTagResourcePermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:TagResource",
      "Resource" : "arn:aws:bedrock:*:*:*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        },
        "StringEqualsIfExists" : {
```

```
          "aws:RequestTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonBedrockManaged",
            "AmazonDataZone*",
            "ProjectUserTag*"
          ]
        }
      }
    },
    {
      "Sid" : "BedrockKmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com"
        },
        "Null" : {
          "kms:EncryptionContext:aws:bedrock:arn" : "false"
        }
      }
    },
    {
      "Sid" : "KmsViaBedrockPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true",
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com"
        },
        "ForAllValues:StringLike" : {
          "kms:EncryptionContextKeys" : [
            "aws:bedrock*:arn",
            "aws:bedrock:guardrail-id"
          ]
        }
      }
    },
    {
      "Sid" : "AccessSecretPermissionsForAmazonBedrockIDE",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:amazon-bedrock-ide/*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SecretsManagerPermissionsForBedrock",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:amazon-bedrock*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
```

```
    },
    {
      "Sid" : "AccessSecretKmsPermissionsForAmazonBedrockIDE",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : "secretsmanager.*.amazonaws.com"
        },
        "ArnLike" : {
          "kms:EncryptionContext:SecretARN" :
"arn:aws:secretsmanager:*:*:secret:amazon-bedrock-ide/*"
        }
      }
    },
    {
      "Sid" : "KmsViaSecretsManagerPermissionsForBedrock",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : "secretsmanager.*.amazonaws.com"
        },
        "ArnLike" : {
          "kms:EncryptionContext:SecretARN" :
"arn:aws:secretsmanager:*:*:secret:amazon-bedrock*"
        }
      }
```

```
    },
    {
      "Sid" : "InvokeFunctionPermissionsForAmazonBedrockIDE",
      "Effect" : "Allow",
      "Action" : "lambda:InvokeFunction",
      "Resource" : "arn:aws:lambda:*:*:function:amazon-bedrock-ide-*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:CalledViaFirst" : "bedrock.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "LambdaInvokeFunctionViaBedrockPermissions",
      "Effect" : "Allow",
      "Action" : "lambda:InvokeFunction",
      "Resource" : "arn:aws:lambda:*:*:function:amazon-bedrock*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:CalledViaFirst" : "bedrock.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "GetDataZoneEnvironmentCloudFormationStackPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:GetTemplate",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/DataZone-Env-*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
```

```
    },
    {
      "Sid" : "CloudFormationGetDataZoneEnvironmentStackPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:GetTemplate"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/DataZone-Env-*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "GetGlueUserDefinedFuncLakeFormationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetUserDefinedFunction",
        "glue:GetUserDefinedFunctions"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:database/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "glue:LakeFormationPermissions" : "Enabled"
        }
      }
    },
    {
      "Sid" : "GetGlueUserDefinedFuncPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetUserDefinedFunction",
        "glue:GetUserDefinedFunctions"
      ],
      "Resource" : [
```

```
        "arn:aws:glue:*:*:userDefinedFunction/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "FederatedConnectionGetSecretPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:*:secretsmanager:*:*:secret:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "FederatedConnectionLambdaLogsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/lambda/athenafederatedcatalog*"
    },
    {
      "Sid" : "FederatedConnectionDDBPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListTables"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "FederatedConnectionEC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
```

```
        "ec2:DescribeSubnets",
        "ec2:DetachNetworkInterface"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:Vpc" : "${aws:PrincipalTag/vpcArn}"
        }
      }
    },
    {
      "Sid" : "FederatedConnectionDeleteENIPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:*/*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "ec2:Vpc" : "${aws:PrincipalTag/vpcArn}"
        }
      }
    },
    {
      "Sid" : "FederatedConnectionDescribeENIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PrivateECRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchCheckLayerAvailability",
        "ecr:CompleteLayerUpload",
        "ecr:DeleteRepository",
        "ecr:InitiateLayerUpload",
        "ecr:PutImage",
        "ecr:BatchDeleteImage",
        "ecr:ListTagsForResource",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "ecr:UploadLayerPart"
      ],
```

```
      "Resource" : "arn:aws:ecr:*:*:repository/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "CreateECRRepositoryPermission",
      "Effect" : "Allow",
      "Action" : "ecr:CreateRepository",
      "Resource" : "arn:aws:ecr:*:*:repository/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "ECRTagResourcePermission",
      "Effect" : "Allow",
      "Action" : "ecr:TagResource",
      "Resource" : "arn:aws:ecr:*:*:repository/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZoneProject",
            "ProjectUserTag*"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        },
        "StringEqualsIfExists" : {
          "aws:RequestTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "ECRUntagResourcePermission",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ecr:UntagResource"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "ProjectUserTag*"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "LakeformationResourceSharingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:BatchGrantPermissions",
        "lakeformation:BatchRevokePermissions",
        "lakeformation:ListPermissions",
        "lakeformation:DescribeResource",
        "ram:GetResourceShareInvitations",
        "lakeformation:CreateDataCellsFilter",
        "lakeformation:ListDataCellsFilter",
        "lakeformation:DeleteDataCellsFilter",
        "lakeformation:GetDataCellsFilter",
        "lakeformation:UpdateDataCellsFilter",
        "ram:ListResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CrossAccountLakeFormationResourceSharingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
```

```
          "ram:RequestedResourceType" : [
            "glue:Table",
            "glue:Database",
            "glue:Catalog"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "lakeformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CrossAccountRAMResourceSharingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:DeleteResourcePolicy",
        "glue:PutResourcePolicy"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "ram.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CrossAccountRAMResourceSharingViaLakeFormationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare",
        "ram:DeleteResourceShare",
        "ram:ListResourceSharePermissions",
        "ram:UpdateResourceShare"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ram:ResourceShareName" : [
            "LakeFormation*"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "lakeformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "RAMGetResourceSharesViaLakeFormation",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShares"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "lakeformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CrossAccountRAMResourceShareInvitationPermission",
      "Effect" : "Allow",
      "Action" : [
        "ram:AcceptResourceShareInvitation"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share-invitation/*",
      "Condition" : {
        "StringLike" : {
          "ram:ResourceShareName" : [
            "LakeFormation*",
            "DataZoneS3AG*"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "CrossAccountRAMResourceSharingViaLakeFormationHybrid",
      "Effect" : "Allow",
      "Action" : "ram:AssociateResourceSharePermission",
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ram:PermissionArn" : "arn:aws:ram::aws:permission/AWSRAMLFEnabled*"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "lakeformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "EventBridgeScheduleActions",
      "Effect" : "Allow",
      "Action" : [
        "scheduler:CreateSchedule",
        "scheduler:GetSchedule",
        "scheduler:UpdateSchedule",
        "scheduler:DeleteSchedule"
      ],
      "Resource" : [
        "arn:aws:scheduler:*:*:schedule/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "EventBridgeScheduleGroupActions",
      "Effect" : "Allow",
      "Action" : [
        "scheduler:GetScheduleGroup"
      ],
      "Resource" : [
        "arn:aws:scheduler:*:*:schedule-group/*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "ManageQuickSightFolderAndDataSourceResources",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeDataSource",
        "quicksight:DescribeFolder",
        "quicksight:DescribeFolderPermissions",
        "quicksight:ListFolderMembers"
      ],
      "Resource" : [
        "arn:aws:quicksight:*:*:folder/*",
        "arn:aws:quicksight:*:*:datasource/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "ManageQuickSightOtherResources",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeDataSet",
        "quicksight:DescribeAccountSubscription",
        "quicksight:DescribeUser",
        "quicksight:DescribeGroup"
      ],
      "Resource" : [
        "arn:aws:quicksight:*:*:*"
      ]
    },
    {
      "Sid" : "ManagePassDataSourcePermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "quicksight:PassDataSource"
      ],
      "Resource" : "arn:aws:quicksight:*:*:datasource/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "ManageCreateDataSetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:CreateDataSet",
        "quicksight:TagResource"
      ],
      "Resource" : "arn:aws:quicksight:*:*:dataset/*",
      "Condition" : {
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        },
        "StringEqualsIfExists" : {
          "aws:RequestTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "CreateFolderMembership",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:CreateFolderMembership"
      ],
```

```
      "Resource" : "arn:aws:quicksight:*:*:folder/sagemaker-*-assets",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceTag/AmazonDataZoneAssetsFolder" : "true"
        }
      }
    },
    {
      "Sid" : "SageMakerUnifiedStudioMcp",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker-unified-studio-mcp:InvokeMcp",
        "sagemaker-unified-studio-mcp:CallReadOnlyTool",
        "sagemaker-unified-studio-mcp:CallPrivilegedTool"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

SageMakerStudioQueryExecutionRolePolicy

説明: Amazon SageMaker Studio は、フェデレーション接続でクエリを実行するときにこのポリシーを使用します。

`SageMakerStudioQueryExecutionRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `SageMakerStudioQueryExecutionRolePolicy` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2025 年 1 月 31 日 19:52 UTC
- 編集日時: 2025 年 9 月 4 日 17:49 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioQueryExecutionRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GlueGetConnectionOnCatalog",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetConnection"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog"
      ]
    },
    {
      "Sid" : "GlueGetConnectionsForProject",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetConnection",
        "glue:GetConnections",
        "glue:GetTags"
      ],
      "Resource" : "arn:aws:glue:*:*:connection/*",
```

```
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "S3GetObjectForAthenaSpillBucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*/dzd*/*/dev/sys/athena/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/SageMakerStudioQueryExecutionRole" : "true"
        }
      }
    },
    {
      "Sid" : "S3ListBucketOwnershipCheckForAthenaSpillBucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::amazon-sagemaker-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/SageMakerStudioQueryExecutionRole" : "true"
        }
      }
    },
    {
      "Sid" : "InvokeFunctionPermissionsForAthenaCatalogLambda",
      "Effect" : "Allow",
      "Action" : "lambda:InvokeFunction",
      "Resource" : "arn:aws:lambda:*:*:function:*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/SageMakerStudioQueryExecutionRole" : "true",
```

```
          "aws:ResourceTag/federated_athena_datacatalog" : "true"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

SageMakerStudioUserIAMConsolePolicy

説明: AWS マネジメントコンソール および SDK を介して Amazon SageMaker Unified Studio の個々のセットアップ権限を提供します。SageMaker Unified Studio Portal の起動を許可します。

`SageMakerStudioUserIAMConsolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `SageMakerStudioUserIAMConsolePolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 8 月 18 日 22:49 UTC
- 編集日時: 2025 年 11 月 14 日 22:49 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioUserIAMConsolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonDataZoneStatement",
      "Effect" : "Allow",
      "Action" : [
        "datazone:ListDomains",
        "datazone:GetDomain",
        "datazone:GetUserProfile",
        "datazone:ListProjects",
        "datazone:ListProjectProfiles",
        "datazone:CreateProject",
        "datazone:GetProject",
        "datazone:DeleteProject",
        "datazone:GetIamPortalLoginUrl",
        "datazone:ListEnvironmentBlueprints",
        "datazone:ListEnvironments",
        "datazone:GetEnvironment",
        "datazone:GetEnvironmentCredentials",
        "datazone:GetGroupProfile",
        "datazone:SearchGroupProfiles",
        "datazone:SearchUserProfiles",
        "datazone:ListProjectMemberships"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ReadOnlyStatement",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "iam:GetRole",
        "iam:GetUser"
      ],
```

```
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DataZoneKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:datazone:domainId"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

SageMakerStudioUserIAMDefaultExecutionPolicy

説明: SageMaker Unified Studio で IAM ロールを使用するための実行ポリシー。SageMaker Unified Studio を IAM ベースで使用するためのローカルアカウントのリソースへのアクセス (データリソースへのアクセスを除く) をユーザーに許可します。

`SageMakerStudioUserIAMDefaultExecutionPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに SageMakerStudioUserIAMDefaultExecutionPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 8 月 18 日 17:19 UTC
- 編集日時: 2025 年 11 月 18 日 23:34 UTC
- ARN: arn:aws:iam::aws:policy/SageMakerStudioUserIAMDefaultExecutionPolicy

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataZone",
      "Effect" : "Allow",
      "Action" : [
        "datazone:AcceptPredictions",
        "datazone:AcceptSubscriptionRequest",
        "datazone:CancelMetadataGenerationRun",
        "datazone:CancelSubscription",
        "datazone:CreateAsset*",
        "datazone:CreateConnection",
        "datazone:CreateEnvironment",
        "datazone:CreateListingChangeSet",
        "datazone:CreateProject",
        "datazone:CreateSubscriptionGrant",
        "datazone:CreateSubscriptionRequest",
```

```
        "datazone:DeleteAsset*",
        "datazone:DeleteConnection",
        "datazone:DeleteEnvironment",
        "datazone:DeleteListing",
        "datazone:DeleteProject",
        "datazone:DeleteSubscriptionGrant",
        "datazone:DeleteSubscriptionRequest",
        "datazone:Get*",
        "datazone:List*",
        "datazone:PostLineageEvent",
        "datazone:RejectPredictions",
        "datazone:RejectSubscriptionRequest",
        "datazone:RevokeSubscription",
        "datazone:Search",
        "datazone:SearchListings",
        "datazone:SearchRules",
        "datazone:SearchTypes",
        "datazone:SearchUserProfiles",
        "datazone:SearchGroupProfiles",
        "datazone:StartMetadataGenerationRun",
        "datazone:UpdateAssetFilter",
        "datazone:UpdateConnection",
        "datazone:UpdateEnvironment",
        "datazone:UpdateProject",
        "datazone:UpdateSubscriptionRequest",
        "datazone:CreateNotebook",
        "datazone:UpdateNotebook",
        "datazone:DeleteNotebook",
        "datazone:CreateCell",
        "datazone:UpdateCell",
        "datazone:DeleteCell",
        "datazone:BatchGetCell",
        "datazone:CreateCellRun",
        "datazone:UpdateCellRun",
        "datazone:DeleteCellRun",
        "datazone:BatchGetCellRun",
        "datazone:PutCellRunResult",
        "datazone:StartNotebookCompute",
        "datazone:StopNotebookCompute",
        "datazone:StartConversation",
        "datazone:GenerateCode",
        "datazone:SendMessage"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "CfnManage",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:*"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*"
      ]
    },
    {
      "Sid" : "ValidateCfn",
      "Effect" : "Allow",
      "Action" : "cloudformation:ValidateTemplate",
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerUnifiedStudioMcp",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker-unified-studio-mcp:InvokeMcp",
        "sagemaker-unified-studio-mcp:CallReadOnlyTool",
        "sagemaker-unified-studio-mcp:CallPrivilegedTool"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IamSts",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRoles",
        "sts:AssumeRole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/neptune-graph.amazonaws.com/
AWSServiceRoleForNeptuneGraph",
```

```
        "arn:aws:iam::*:role/aws-service-role/redshift.amazonaws.com/
AWSServiceRoleForRedshift",
        "arn:aws:iam::*:role/aws-service-role/sagemaker.amazonaws.com/
AWSServiceRoleForAmazonSageMakerNotebooks",
        "arn:aws:iam::*:role/aws-service-role/ops.emr-serverless.amazonaws.com/
AWSServiceRoleForAmazonEMRServerless",
        "arn:aws:iam::*:role/aws-service-role/airflow.amazonaws.com/
AWSServiceRoleForAmazonMWAA",
        "arn:aws:iam::*:role/aws-service-role/airflow-serverless.amazonaws.com/
AWSServiceRoleForAmazonMWAAServerless",
        "arn:aws:iam::*:role/aws-service-role/elasticmapreduce.amazonaws.com/
AWSServiceRoleForEMRCleanup",
        "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
        "arn:aws:iam::*:role/aws-service-role/observability.aoss.amazonaws.com/
AWSServiceRoleForAmazonOpenSearchServerless"
      ]
    },
    {
      "Sid" : "TagSession",
      "Effect" : "Allow",
      "Action" : "sts:TagSession",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        }
      }
    },
    {
      "Sid" : "SourceIdentity",
      "Effect" : "Allow",
      "Action" : "sts:SetSourceIdentity",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "sts:SourceIdentity" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "Q",
```

```
      "Effect" : "Allow",
      "Action" : [
        "glue:StartCompletion",
        "q:Get*",
        "q:List*",
        "q:PassRequest",
        "q:SendMessage",
        "q:StartConversation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSM",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter*"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/amazon/datazone/q*",
        "arn:aws:ssm:*:*:parameter/amazon/datazone/genAI/*",
        "arn:aws:ssm:*::parameter/aws/service/sagemaker-distribution/*"
      ]
    },
    {
      "Sid" : "SageMakerUserTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreatePresignedDomainUrl",
        "sagemaker:CreateUserProfile",
        "sagemaker:DeleteUserProfile"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:user-profile/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneUser" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "SageMakerPrivateSpace",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateApp",
        "sagemaker:CreateSpace",
```

```
        "sagemaker:DeleteApp",
        "sagemaker:DeleteSpace",
        "sagemaker:UpdateSpace"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:space/*",
        "arn:aws:sagemaker:*:*:app/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneUser" : "${aws:PrincipalTag/datazone:userId}",
          "sagemaker:SpaceSharingType" : [
            "Private"
          ]
        }
      }
    },
    {
      "Sid" : "AllowStartSessionForSpaceRemoteConnection",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:StartSession"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:space/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneUser" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "ResourceGroupsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:GetGroupQuery",
        "resource-groups:ListGroupResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:Batch*",
```

```
        "sagemaker:Describe*",
        "sagemaker:List*",
        "sagemaker:Search",
        "sagemaker:*Endpoint*",
        "sagemaker:*Model*",
        "sagemaker:*Context*",
        "sagemaker:*Artifact*",
        "sagemaker:*Action*",
        "sagemaker:*Association*",
        "sagemaker:QueryLineage",
        "sagemaker:*InferenceComponent*",
        "sagemaker:*Job*",
        "sagemaker:StartMlflowTrackingServer",
        "sagemaker:StopMlflowTrackingServer",
        "sagemaker:CreatePresignedMlflowTrackingServerUrl",
        "sagemaker-mlflow:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags",
        "sagemaker:DeleteTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringNotLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "sagemaker:shared-with:*"
          ]
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "ProjectUserTag*",
            "sagemaker*",
            "sm-jumpstart*",
            "endpoint-has-jumpstart-model"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "LogsAndMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:Describe*",
        "logs:Get*",
        "logs:PutLogEvents",
        "logs:StopQuery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Glue",
      "Effect" : "Allow",
      "Action" : [
        "glue:CancelStatement",
        "glue:CreateSession",
        "glue:DeleteSession",
        "glue:CreateCatalog",
        "glue:Describe*",
        "glue:Get*",
        "glue:List*",
        "glue:NotifyEvent",
        "glue:RunStatement",
        "glue:StartCompletion",
        "glue:StopSession",
        "glue:UseGlueStudio",
        "glue:TagResource",
        "glue:UntagResource",
        "glue:*Job*",
        "glue:TestConnection"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueSessionIsolation",
      "Effect" : "Deny",
      "Action" : [
        "glue:CancelStatement",
        "glue:CreateSession",
        "glue:DeleteSession",
```

```
        "glue:GetSession",
        "glue:GetStatement",
        "glue:RunStatement",
        "glue:StopSession",
        "glue:GetDashboardUrl"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:RequestTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}",
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
      }
    },
    {
      "Sid" : "DenyTaggingUntaggingForeignSessions",
      "Effect" : "Deny",
      "Action" : [
        "glue:TagResource",
        "glue:UntagResource"
      ],
      "Resource" : "arn:aws:glue:*:*:session/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
      }
    },
    {
      "Sid" : "GlueDatabase",
      "Effect" : "Allow",
      "Action" : [
        "glue:*"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*"
      ]
    },
    {
```

```
      "Sid" : "GlueLakeFormation",
      "Effect" : "Allow",
      "Action" : [
        "glue:*"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "glue:LakeFormationPermissions" : "Enabled"
        }
      }
    },
    {
      "Sid" : "LFAccess",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:BatchGrantPermissions",
        "lakeformation:BatchRevokePermissions",
        "lakeformation:DescribeResource",
        "lakeformation:GetDataAccess",
        "lakeformation:GrantPermissions",
        "lakeformation:ListResources",
        "lakeformation:ListPermissions",
        "lakeformation:RevokePermissions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SQLWorkBench",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftData",
      "Effect" : "Allow",
      "Action" : "redshift-data:*",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "redshift-data:statement-owner-iam-userid" : "${aws:userid}"
        }
```

```
      }
    },
    {
      "Sid" : "RedShiftActions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:BatchExecuteStatement",
        "redshift-data:Describe*",
        "redshift-data:ExecuteStatement",
        "redshift-data:List*",
        "redshift-serverless:GetManagedWorkgroup",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:List*",
        "redshift:Describe*",
        "redshift:GetClusterCredentialsWithIAM",
        "redshift-serverless:GetCredentials"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Bedrock",
      "Effect" : "Allow",
      "Action" : "bedrock:*",
      "Resource" : "*"
    },
    {
      "Sid" : "PassRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/${aws:PrincipalTag/
AmazonDataZonePassedRolePath}",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "bedrock.amazonaws.com",
            "glue.amazonaws.com",
            "lakeformation.amazonaws.com",
            "sagemaker.amazonaws.com",
            "scheduler.amazonaws.com",
            "emr-serverless.amazonaws.com",
            "redshift.amazonaws.com",
```

```
            "airflow-serverless.amazonaws.com"
          ],
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AirflowServerless",
      "Effect" : "Allow",
      "Action" : [
        "airflow-serverless:List*",
        "airflow-serverless:Get*",
        "airflow-serverless:CreateWorkflow",
        "airflow-serverless:UpdateWorkflow",
        "airflow-serverless:DeleteWorkflow",
        "airflow-serverless:StartWorkflowRun",
        "airflow-serverless:StopWorkflowRun",
        "airflow-serverless:TagResource",
        "airflow-serverless:UntagResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3List",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketAcl",
        "s3:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3CrossAccount",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject*"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
```

```
    {
      "Sid" : "Scheduler",
      "Effect" : "Allow",
      "Action" : [
        "scheduler:CreateSchedule",
        "scheduler:DeleteSchedule",
        "scheduler:Get*",
        "scheduler:List*",
        "scheduler:UpdateSchedule"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "FederatedConn",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:List*",
        "dynamodb:Describe*",
        "dynamodb:Scan",
        "dynamodb:PartiQLSelect",
        "dynamodb:Query",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Athena",
      "Effect" : "Allow",
      "Action" : [
        "athena:BatchGet*",
        "athena:CreateNamedQuery",
        "athena:CreateNotebook",
        "athena:CreatePreparedStatement",
        "athena:CreatePresignedNotebookUrl",
        "athena:DeleteNamedQuery",
        "athena:DeleteNotebook",
        "athena:DeletePreparedStatement",
        "athena:ExportNotebook",
        "athena:Get*",
        "athena:ImportNotebook",
        "athena:List*",
        "athena:StartCalculationExecution",
        "athena:StartQueryExecution",
        "athena:StartSession",
```

```
        "athena:StopCalculationExecution",
        "athena:StopQueryExecution",
        "athena:TagResource",
        "athena:TerminateSession",
        "athena:UpdateNamedQuery",
        "athena:UpdateNotebook",
        "athena:UpdateNotebookMetadata",
        "athena:UpdatePreparedStatement"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AthenaSessionIsolation",
      "Effect" : "Deny",
      "Action" : [
        "athena:StartSession",
        "athena:GetSession",
        "athena:TerminateSession",
        "athena:GetSessionStatus",
        "athena:GetSessionEndpoint",
        "athena:GetResourceDashboard"
      ],
      "Resource" : [
        "arn:aws:athena:*:*:workgroup/*/session/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:RequestTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}",
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
      }
    },
    {
      "Sid" : "DenyTaggingUntaggingForeignAthenaSessions",
      "Effect" : "Deny",
      "Action" : [
        "athena:TagResource",
        "athena:UntagResource"
      ],
      "Resource" : "arn:aws:athena:*:*:workgroup/*/session/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
```

```
      }
    },
    {
      "Sid" : "PrivateSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:UpdateSecret",
        "secretsmanager:PutResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${datazone:projectId}"
        }
      }
    },
    {
      "Sid" : "SharedSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:UpdateSecret"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "GenerateRecommendations",
      "Effect" : "Allow",
      "Action" : [
        "codewhisperer:GenerateRecommendations"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "Ecr",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:DescribeImages",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeConnectionsUser",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:UseConnection",
        "codeconnections:ListConnections",
        "codeconnections:GetConnection",
        "codeconnections:GetHost",
        "codeconnections:ListTagsForResource",
        "codestar-connections:UseConnection",
        "codestar-connections:ListConnections",
        "codestar-connections:GetConnection",
        "codestar-connections:GetHost",
        "codestar-connections:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KmsListAndDescribe",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListGrants"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataZoneKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
```

```
        "kms:GenerateDataKey",
        "kms:Encrypt",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:datazone:domainId"
        }
      }
    },
    {
      "Sid" : "S3Kms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "Null" : {
          "kms:EncryptionContext:aws:s3:arn" : "false"
        }
      }
    },
    {
      "Sid" : "SchedulerKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:scheduler:schedule:arn" : "false"
```

```
        }
      }
    },
    {
      "Sid" : "SecretsKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "secretsmanager.*.amazonaws.com"
        },
        "Null" : {
          "kms:EncryptionContext:SecretARN" : "false"
        }
      }
    },
    {
      "Sid" : "SageMakerKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "sagemaker.*.amazonaws.com"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "SageMakerCreateGrant",
```

```
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "sagemaker.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DataZoneCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Encrypt",
            "Decrypt",
            "ReEncryptFrom",
            "ReEncryptTo",
            "GenerateDataKeyWithoutPlaintext",
            "GenerateDataKey",
            "DescribeKey",
            "RetireGrant",
            "CreateGrant"
          ]
        }
      }
    },
    {
      "Sid" : "GlueKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
```

```
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "glue.*.amazonaws.com"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "BedrockKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "WorkflowsCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:*:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "airflow-serverless.*.amazonaws.com"
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:airflow-serverless:workflow-arn"
        },
```

```
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt",
            "Encrypt",
            "GenerateDataKey",
            "GenerateDataKeyWithoutPlaintext",
            "RetireGrant"
          ]
        }
      }
    },
    {
      "Sid" : "WorkflowsKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:*:kms:*:*:key/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:airflow-serverless:workflow-arn"
        }
      }
    },
    {
      "Sid" : "Ec2DescribeOnly",
      "Effect" : "Allow",
      "Action" : "ec2:Describe*",
      "Resource" : "*"
    },
    {
      "Sid" : "VpcAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "EC2TagAccessForVpc",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    },
    {
      "Sid" : "AccessProjectS3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject*",
        "s3:PutObject*",
        "s3:RestoreObject",
        "s3:ReplicateObject",
        "s3:DeleteObject*",
        "s3:ListMultipartUploadParts",
        "s3:AbortMultipartUpload"
      ],
      "Resource" : [
        "arn:aws:s3:::${aws:PrincipalTag/AmazonDataZoneProjectBucket}/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/AmazonDataZoneProjectBucket" : ""
        }
      }
    },
    {
      "Sid" : "EMRServerless",
      "Effect" : "Allow",
      "Action" : [
        "emr-serverless:ListApplications",
        "emr-serverless:GetApplication"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

SageMakerStudioUserIAMPermissiveExecutionPolicy

説明: SageMaker Unified Studio で IAM ロールを使用するための実行ポリシー。SageMaker Unified Studio を IAM ベースで使用するために、アカウント内のリソースにユーザーがアクセスできるようにします (S3、Glue、CloudWatch Logs などのデータサービス内のすべての API への広範なアクセスを含む)。

`SageMakerStudioUserIAMPermissiveExecutionPolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `SageMakerStudioUserIAMPermissiveExecutionPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 8 月 18 日 17:19 UTC
- 編集日時: 2025 年 11 月 18 日 23:34 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioUserIAMPermissiveExecutionPolicy`

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:*",
        "glue:*",
        "logs:*",
        "redshift-data:*",
        "redshift-serverless:*",
        "redshift:*",
        "s3:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ComputeAccess",
      "Effect" : "Allow",
      "Action" : [
        "athena:*",
        "bedrock:*",
        "codewhisperer:*",
        "sagemaker-unified-studio-mcp:*",
        "q:*",
        "sagemaker:*",
        "sagemaker-mlflow:*",
        "scheduler:*",
        "sqlworkbench:*",
        "emr-serverless:*",
        "airflow-serverless:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueSessionIsolation",
      "Effect" : "Deny",
      "Action" : [
        "glue:CancelStatement",
        "glue:CreateSession",
```

```
        "glue:DeleteSession",
        "glue:GetSession",
        "glue:GetStatement",
        "glue:RunStatement",
        "glue:StopSession",
        "glue:GetDashboardUrl"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:RequestTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}",
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
      }
    },
    {
      "Sid" : "DenyTaggingUntaggingForeignSessions",
      "Effect" : "Deny",
      "Action" : [
        "glue:TagResource",
        "glue:UntagResource"
      ],
      "Resource" : "arn:aws:glue:*:*:session/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
      }
    },
    {
      "Sid" : "DataZone",
      "Effect" : "Allow",
      "Action" : [
        "datazone:AcceptPredictions",
        "datazone:AcceptSubscriptionRequest",
        "datazone:CancelMetadataGenerationRun",
        "datazone:CancelSubscription",
        "datazone:CreateAsset*",
        "datazone:CreateConnection",
        "datazone:CreateEnvironment",
        "datazone:CreateListingChangeSet",
        "datazone:CreateProject",
```

```
        "datazone:CreateSubscriptionGrant",
        "datazone:CreateSubscriptionRequest",
        "datazone:DeleteAsset*",
        "datazone:DeleteConnection",
        "datazone:DeleteEnvironment",
        "datazone:DeleteListing",
        "datazone:DeleteProject",
        "datazone:DeleteSubscriptionGrant",
        "datazone:DeleteSubscriptionRequest",
        "datazone:Get*",
        "datazone:List*",
        "datazone:PostLineageEvent",
        "datazone:RejectPredictions",
        "datazone:RejectSubscriptionRequest",
        "datazone:RevokeSubscription",
        "datazone:Search",
        "datazone:SearchListings",
        "datazone:SearchRules",
        "datazone:SearchTypes",
        "datazone:SearchUserProfiles",
        "datazone:SearchGroupProfiles",
        "datazone:StartMetadataGenerationRun",
        "datazone:UpdateAssetFilter",
        "datazone:UpdateConnection",
        "datazone:UpdateEnvironment",
        "datazone:UpdateProject",
        "datazone:UpdateSubscriptionRequest",
        "datazone:CreateNotebook",
        "datazone:UpdateNotebook",
        "datazone:DeleteNotebook",
        "datazone:CreateCell",
        "datazone:UpdateCell",
        "datazone:DeleteCell",
        "datazone:BatchGetCell",
        "datazone:CreateCellRun",
        "datazone:UpdateCellRun",
        "datazone:DeleteCellRun",
        "datazone:BatchGetCellRun",
        "datazone:PutCellRunResult",
        "datazone:StartNotebookCompute",
        "datazone:StopNotebookCompute",
        "datazone:StartConversation",
        "datazone:GenerateCode",
        "datazone:SendMessage"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CfnManage",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:*"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*"
      ]
    },
    {
      "Sid" : "ValidateCfn",
      "Effect" : "Allow",
      "Action" : "cloudformation:ValidateTemplate",
      "Resource" : "*"
    },
    {
      "Sid" : "IamSts",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRoles",
        "sts:AssumeRole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/neptune-graph.amazonaws.com/
AWSServiceRoleForNeptuneGraph",
        "arn:aws:iam::*:role/aws-service-role/redshift.amazonaws.com/
AWSServiceRoleForRedshift",
        "arn:aws:iam::*:role/aws-service-role/sagemaker.amazonaws.com/
AWSServiceRoleForAmazonSageMakerNotebooks",
        "arn:aws:iam::*:role/aws-service-role/ops.emr-serverless.amazonaws.com/
AWSServiceRoleForAmazonEMRServerless",
        "arn:aws:iam::*:role/aws-service-role/airflow.amazonaws.com/
AWSServiceRoleForAmazonMWAA",
```

```
        "arn:aws:iam::*:role/aws-service-role/airflow-serverless.amazonaws.com/
AWSServiceRoleForAmazonMWAAServerless",
        "arn:aws:iam::*:role/aws-service-role/elasticmapreduce.amazonaws.com/
AWSServiceRoleForEMRCleanup",
        "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
        "arn:aws:iam::*:role/aws-service-role/observability.aoss.amazonaws.com/
AWSServiceRoleForAmazonOpenSearchServerless"
      ]
    },
    {
      "Sid" : "TagSession",
      "Effect" : "Allow",
      "Action" : "sts:TagSession",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        }
      }
    },
    {
      "Sid" : "PassRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSageMaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com",
            "lakeformation.amazonaws.com",
            "glue.amazonaws.com",
            "bedrock.amazonaws.com",
            "redshift-serverless.amazonaws.com",
            "redshift.amazonaws.com",
            "scheduler.amazonaws.com",
            "emr-serverless.amazonaws.com",
            "airflow-serverless.amazonaws.com"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "SourceIdentity",
      "Effect" : "Allow",
      "Action" : "sts:SetSourceIdentity",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "sts:SourceIdentity" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "SSM",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter*"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/amazon/datazone/q*",
        "arn:aws:ssm:*:*:parameter/amazon/datazone/genAI/*",
        "arn:aws:ssm:*::parameter/aws/service/sagemaker-distribution/*"
      ]
    },
    {
      "Sid" : "LFAccess",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:BatchGrantPermissions",
        "lakeformation:BatchRevokePermissions",
        "lakeformation:DescribeResource",
        "lakeformation:GetDataAccess",
        "lakeformation:GrantPermissions",
        "lakeformation:ListResources",
        "lakeformation:ListPermissions",
        "lakeformation:RevokePermissions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "FederatedConn",
      "Effect" : "Allow",
      "Action" : [
```

```
        "dynamodb:List*",
        "dynamodb:Describe*",
        "dynamodb:Scan",
        "dynamodb:PartiQLSelect",
        "dynamodb:Query",
        "secretsmanager:ListSecrets",
        "resource-groups:GetGroupQuery",
        "resource-groups:ListGroupResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PrivateSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:UpdateSecret",
        "secretsmanager:PutResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${datazone:projectId}"
        }
      }
    },
    {
      "Sid" : "SharedSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:UpdateSecret"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
```

```
    },
    {
      "Sid" : "Ecr",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:DescribeImages",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeConnectionsUser",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:UseConnection",
        "codeconnections:ListConnections",
        "codeconnections:GetConnection",
        "codeconnections:GetHost",
        "codeconnections:ListTagsForResource",
        "codestar-connections:UseConnection",
        "codestar-connections:ListConnections",
        "codestar-connections:GetConnection",
        "codestar-connections:GetHost",
        "codestar-connections:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KmsListAndDescribe",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListGrants"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataZoneKms",
      "Effect" : "Allow",
      "Action" : [
```

```
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "kms:Encrypt",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:datazone:domainId"
        }
      }
    },
    {
      "Sid" : "S3Kms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "Null" : {
          "kms:EncryptionContext:aws:s3:arn" : "false"
        }
      }
    },
    {
      "Sid" : "SchedulerKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
```

```
          "kms:EncryptionContext:aws:scheduler:schedule:arn" : "false"
        }
      }
    },
    {
      "Sid" : "SecretsKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "secretsmanager.*.amazonaws.com"
        },
        "Null" : {
          "kms:EncryptionContext:SecretARN" : "false"
        }
      }
    },
    {
      "Sid" : "SageMakerKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "sagemaker.*.amazonaws.com"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
```

```
      "Sid" : "SageMakerCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "sagemaker.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DataZoneCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Encrypt",
            "Decrypt",
            "ReEncryptFrom",
            "ReEncryptTo",
            "GenerateDataKeyWithoutPlaintext",
            "GenerateDataKey",
            "DescribeKey",
            "RetireGrant",
            "CreateGrant"
          ]
        }
      }
    },
    {
      "Sid" : "GlueKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
```

```
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "glue.*.amazonaws.com"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "BedrockKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "WorkflowsCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:*:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "airflow-serverless.*.amazonaws.com"
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:airflow-serverless:workflow-arn"
```

```
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt",
            "Encrypt",
            "GenerateDataKey",
            "GenerateDataKeyWithoutPlaintext",
            "RetireGrant"
          ]
        }
      }
    },
    {
      "Sid" : "WorkflowsKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:*:kms:*:*:key/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:airflow-serverless:workflow-arn"
        }
      }
    },
    {
      "Sid" : "Ec2DescribeOnly",
      "Effect" : "Allow",
      "Action" : "ec2:Describe*",
      "Resource" : "*"
    },
    {
      "Sid" : "VpcAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "EC2TagAccessForVpc",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    },
    {
      "Sid" : "AthenaSessionIsolation",
      "Effect" : "Deny",
      "Action" : [
        "athena:StartSession",
        "athena:GetSession",
        "athena:TerminateSession",
        "athena:GetSessionStatus",
        "athena:GetSessionEndpoint",
        "athena:GetResourceDashboard"
      ],
      "Resource" : [
        "arn:aws:athena:*:*:workgroup/*/session/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:RequestTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}",
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
      }
    },
    {
      "Sid" : "DenyTaggingUntaggingForeignAthenaSessions",
      "Effect" : "Deny",
      "Action" : [
        "athena:TagResource",
        "athena:UntagResource"
      ],
      "Resource" : "arn:aws:athena:*:*:workgroup/*/session/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
```

```
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

SecretsManagerReadWrite

説明: 経由で AWS Secrets Manager への読み取り/書き込みアクセスを提供します AWS マネジメントコンソール。注: これには IAM アクションは含まれないため、ローテーション設定が必要な場合は IAMFullAccess と組み合わせてください。

`SecretsManagerReadWrite` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `SecretsManagerReadWrite` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 4 月 4 日 18:05 UTC
- 編集日時: 2024 年 2 月 22 日 18:12 UTC
- ARN: `arn:aws:iam::aws:policy/SecretsManagerReadWrite`

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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-*/*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

SecurityAgentWebAppAPIPolicy

説明: 認証されたユーザーが Security Agent ウェブアプリケーションにアクセスして、自動セキュリティ侵入テストを設定および実行するためのアクセス許可を提供します。このポリシーにより、ユー

ザーはペンテストの管理、結果の表示、テストの実行のモニタリング、セキュリティテストオペレーションに必要な AWS リソースの操作を行うことができます。

SecurityAgentWebAppAPIPolicy は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに SecurityAgentWebAppAPIPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2025 年 12 月 2 日 15:04 UTC
- 編集日時: 2025 年 12 月 10 日 01:04 UTC
- ARN: arn:aws:iam::aws:policy/service-role/SecurityAgentWebAppAPIPolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ApplicationAccess",
      "Effect" : "Allow",
      "Action" : [
        "securityagent:ListAgentInstances",
        "securityagent:ListControls"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Sid" : "AgentInstanceAccess",
      "Effect" : "Allow",
      "Action" : [
        "securityagent:AddArtifact",
        "securityagent:BatchDeletePentests",
        "securityagent:BatchGetAgentInstances",
        "securityagent:BatchGetArtifactMetadata",
        "securityagent:BatchGetFindings",
        "securityagent:BatchGetPentestJobs",
        "securityagent:BatchGetPentests",
        "securityagent:BatchGetSecurityTestContentMetadata",
        "securityagent:BatchGetTasks",
        "securityagent:CreateDocumentReview",
        "securityagent:CreatePentest",
        "securityagent:DeleteArtifact",
        "securityagent:GetArtifact",
        "securityagent:GetCodeReviewTask",
        "securityagent:GetDocReviewTask",
        "securityagent:GetDocumentReview",
        "securityagent:GetDocumentReviewArtifact",
        "securityagent:ListArtifacts",
        "securityagent:ListControls",
        "securityagent:ListDiscoveredEndpoints",
        "securityagent:ListDocumentReviewComments",
        "securityagent:ListDocumentReviews",
        "securityagent:ListFindings",
        "securityagent:ListIntegratedResources",
        "securityagent:ListPentestJobsForPentest",
        "securityagent:ListPentests",
        "securityagent:ListTasks",
        "securityagent:StartPentestExecution",
        "securityagent:StopPentestExecution",
        "securityagent:UpdateFinding",
        "securityagent:UpdatePentest"
      ],
      "Resource" : "arn:aws:securityagent:*:*:agent-instance*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

SecurityAudit

説明: セキュリティ監査テンプレートは、セキュリティ設定メタデータを読み取るためのアクセス権を付与します。 AWS アカウントの設定を監査するソフトウェアに便利です。

`SecurityAudit` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `SecurityAudit` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2025 年 10 月 13 日 18:19 UTC
- ARN: `arn:aws:iam::aws:policy/SecurityAudit`

ポリシーのバージョン

ポリシーのバージョン: v56 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BaseSecurityAuditStatement",
      "Effect" : "Allow",
      "Action" : [
        "a4b:ListSkills",
        "access-analyzer:GetAnalyzedResource",
        "access-analyzer:GetAnalyzer",
        "access-analyzer:GetArchiveRule",
        "access-analyzer:GetFinding",
        "access-analyzer:ListAnalyzedResources",
        "access-analyzer:ListAnalyzers",
        "access-analyzer:ListArchiveRules",
        "access-analyzer:ListFindings",
        "access-analyzer:ListTagsForResource",
        "account:GetAccountInformation",
        "account:GetAlternateContact",
        "account:GetPrimaryEmail",
        "account:GetRegionOptStatus",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:DescribeCertificateAuthorityAuditReport",
        "acm-pca:GetPolicy",
        "acm-pca:ListCertificateAuthorities",
        "acm-pca:ListPermissions",
        "acm-pca:ListTags",
        "acm:Describe*",
        "acm:List*",
        "airflow:GetEnvironment",
        "airflow:ListEnvironments",
        "appflow:ListFlows",
        "appflow:ListTagsForResource",
        "application-autoscaling:Describe*",
        "appmesh:Describe*",
        "appmesh:List*",
        "apprunner:DescribeAutoScalingConfiguration",
        "apprunner:DescribeCustomDomains",
        "apprunner:DescribeObservabilityConfiguration",
        "apprunner:DescribeService",
        "apprunner:DescribeVpcConnector",
```

```
        "apprunner:DescribeVpcIngressConnection",
        "apprunner:ListAutoScalingConfigurations",
        "apprunner:ListConnections",
        "apprunner:ListObservabilityConfigurations",
        "apprunner:ListOperations",
        "apprunner:ListServices",
        "apprunner:ListTagsForResource",
        "apprunner:ListVpcConnectors",
        "apprunner:ListVpcIngressConnections",
        "appsync:GetApiCache",
        "appsync:List*",
        "athena:GetWorkGroup",
        "athena:List*",
        "auditmanager:GetAccountStatus",
        "auditmanager:ListAssessmentControlInsightsByControlDomain",
        "auditmanager:ListAssessmentFrameworks",
        "auditmanager:ListAssessmentFrameworkShareRequests",
        "auditmanager:ListAssessmentReports",
        "auditmanager:ListAssessments",
        "auditmanager:ListControlDomainInsights",
        "auditmanager:ListControlDomainInsightsByAssessment",
        "auditmanager:ListControlInsightsByControlDomain",
        "auditmanager:ListControls",
        "auditmanager:ListNotifications",
        "auditmanager:ListTagsForResource",
        "autoscaling-plans:DescribeScalingPlans",
        "autoscaling:Describe*",
        "backup:DescribeGlobalSettings",
        "backup:DescribeRegionSettings",
        "backup:GetBackupVaultAccessPolicy",
        "backup:GetBackupVaultNotifications",
        "backup:ListBackupVaults",
        "backup:ListTags",
        "batch:DescribeComputeEnvironments",
        "batch:DescribeJobDefinitions",
        "bedrock:GetAgentAlias",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:GetCustomModel",
        "bedrock:GetFlowAlias",
        "bedrock:GetFoundationModel",
        "bedrock:GetFoundationModelAvailability",
        "bedrock:GetImportedModel",
        "bedrock:GetInferenceProfile",
        "bedrock:GetIngestionJob",
```

```
        "bedrock:GetKnowledgeBaseDocuments",
        "bedrock:GetMarketplaceModelEndpoint",
        "bedrock:GetModelCopyJob",
        "bedrock:GetModelCustomizationJob",
        "bedrock:GetModelImportJob",
        "bedrock:GetModelInvocationLoggingConfiguration",
        "bedrock:GetPromptRouter",
        "bedrock:GetProvisionedModelThroughput",
        "bedrock:ListAgentActionGroups",
        "bedrock:ListAgentAliases",
        "bedrock:ListAgentKnowledgeBases",
        "bedrock:ListAgents",
        "bedrock:ListAgentVersions",
        "bedrock:ListCustomModels",
        "bedrock:ListDataSources",
        "bedrock:ListEvaluationJobs",
        "bedrock:ListFlowAliases",
        "bedrock:ListFlows",
        "bedrock:ListFlowVersions",
        "bedrock:ListFoundationModels",
        "bedrock:ListGuardrails",
        "bedrock:ListImportedModels",
        "bedrock:ListInferenceProfiles",
        "bedrock:ListIngestionJobs",
        "bedrock:ListKnowledgeBases",
        "bedrock:ListMarketplaceModelEndpoints",
        "bedrock:ListModelCopyJobs",
        "bedrock:ListModelCustomizationJobs",
        "bedrock:ListModelImportJobs",
        "bedrock:ListModelInvocationJobs",
        "bedrock:ListPromptRouters",
        "bedrock:ListPrompts",
        "bedrock:ListProvisionedModelThroughputs",
        "bedrock:ListTagsForResource",
        "braket:SearchJobs",
        "braket:SearchQuantumTasks",
        "chime:List*",
        "cleanrooms:BatchGetCollaborationAnalysisTemplate",
        "cleanrooms:BatchGetSchema",
        "cleanrooms:BatchGetSchemaAnalysisRule",
        "cleanrooms:GetAnalysisTemplate",
        "cleanrooms:GetCollaboration",
        "cleanrooms:GetCollaborationAnalysisTemplate",
        "cleanrooms:GetCollaborationConfiguredAudienceModelAssociation",
```

```
        "cleanrooms:GetCollaborationIdNamespaceAssociation",
        "cleanrooms:GetCollaborationPrivacyBudgetTemplate",
        "cleanrooms:GetConfiguredAudienceModelAssociation",
        "cleanrooms:GetConfiguredTable",
        "cleanrooms:GetConfiguredTableAnalysisRule",
        "cleanrooms:GetConfiguredTableAssociation",
        "cleanrooms:GetConfiguredTableAssociationAnalysisRule",
        "cleanrooms:GetIdMappingTable",
        "cleanrooms:GetIdNamespaceAssociation",
        "cleanrooms:GetMembership",
        "cleanrooms:GetPrivacyBudgetTemplate",
        "cleanrooms:GetProtectedQuery",
        "cleanrooms:GetSchema",
        "cleanrooms:GetSchemaAnalysisRule",
        "cleanrooms:ListAnalysisTemplates",
        "cleanrooms:ListCollaborationAnalysisTemplates",
        "cleanrooms:ListCollaborationConfiguredAudienceModelAssociations",
        "cleanrooms:ListCollaborationIdNamespaceAssociations",
        "cleanrooms:ListCollaborationPrivacyBudgetTemplates",
        "cleanrooms:ListCollaborationPrivacyBudgets",
        "cleanrooms:ListCollaborations",
        "cleanrooms:ListConfiguredAudienceModelAssociations",
        "cleanrooms:ListConfiguredTableAssociations",
        "cleanrooms:ListConfiguredTables",
        "cleanrooms:ListIdMappingTables",
        "cleanrooms:ListIdNamespaceAssociations",
        "cleanrooms:ListMembers",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListPrivacyBudgetTemplates",
        "cleanrooms:ListPrivacyBudgets",
        "cleanrooms:ListProtectedQueries",
        "cleanrooms:ListSchemas",
        "cleanrooms:ListTagsForResource",
        "cleanrooms:PreviewPrivacyImpact",
        "cloud9:Describe*",
        "cloud9:ListEnvironments",
        "clouddirectory:ListDirectories",
        "cloudformation:DescribeStack*",
        "cloudformation:GetStackPolicy",
        "cloudformation:GetTemplate",
        "cloudformation:ListStack*",
        "cloudfront:Get*",
        "cloudfront:List*",
        "cloudsearch:DescribeDomainEndpointOptions",
```

```
        "cloudsearch:DescribeDomains",
        "cloudsearch:DescribeServiceAccessPolicies",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetEventSelectors",
        "cloudtrail:GetInsightSelectors",
        "cloudtrail:GetTrail",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:ListTags",
        "cloudtrail:ListTrails",
        "cloudtrail:LookupEvents",
        "cloudwatch:Describe*",
        "cloudwatch:GetDashboard",
        "cloudwatch:ListDashboards",
        "cloudwatch:ListTagsForResource",
        "codeartifact:GetDomainPermissionsPolicy",
        "codeartifact:GetRepositoryPermissionsPolicy",
        "codeartifact:ListRepositories",
        "codebuild:BatchGetProjects",
        "codebuild:GetResourcePolicy",
        "codebuild:ListProjects",
        "codebuild:ListSourceCredentials",
        "codecommit:BatchGetRepositories",
        "codecommit:GetBranch",
        "codecommit:GetObjectIdentifier",
        "codecommit:GetRepository",
        "codecommit:GetRepositoryTriggers",
        "codecommit:List*",
        "codedeploy:Batch*",
        "codedeploy:Get*",
        "codedeploy:List*",
        "codepipeline:GetJobDetails",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineExecution",
        "codepipeline:GetPipelineState",
        "codepipeline:ListPipelines",
        "codestar:Describe*",
        "codestar:List*",
        "cognito-identity:Describe*",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:ListIdentityPools",
        "cognito-identity:ListTagsForResource",
        "cognito-idp:Describe*",
        "cognito-idp:ListDevices",
        "cognito-idp:ListGroups",
```

```
        "cognito-idp:ListIdentityProviders",
        "cognito-idp:ListResourceServers",
        "cognito-idp:ListTagsForResource",
        "cognito-idp:ListUserImportJobs",
        "cognito-idp:ListUserPoolClients",
        "cognito-idp:ListUserPools",
        "cognito-idp:ListUsers",
        "cognito-idp:ListUsersInGroup",
        "cognito-sync:Describe*",
        "cognito-sync:List*",
        "comprehend:Describe*",
        "comprehend:List*",
        "comprehendmedical:ListICD10CMInferenceJobs",
        "comprehendmedical:ListPHIDetectionJobs",
        "comprehendmedical:ListRxNormInferenceJobs",
        "comprehendmedical:ListSNOMEDCTInferenceJobs",
        "config:BatchGetAggregateResourceConfig",
        "config:BatchGetResourceConfig",
        "config:Deliver*",
        "config:Describe*",
        "config:Get*",
        "config:List*",
        "config:SelectAggregateResourceConfig",
        "config:SelectResourceConfig",
        "connect:ListApprovedOrigins",
        "connect:ListInstanceAttributes",
        "connect:ListInstances",
        "connect:ListInstanceStorageConfigs",
        "connect:ListIntegrationAssociations",
        "connect:ListLambdaFunctions",
        "connect:ListLexBots",
        "connect:ListSecurityKeys",
        "databrew:DescribeDataset",
        "databrew:DescribeProject",
        "databrew:ListJobs",
        "databrew:ListProjects",
        "dataexchange:ListDataSets",
        "datapipeline:DescribeObjects",
        "datapipeline:DescribePipelines",
        "datapipeline:EvaluateExpression",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:ListPipelines",
        "datapipeline:QueryObjects",
        "datapipeline:ValidatePipelineDefinition",
```

```
        "datasync:Describe*",
        "datasync:List*",
        "dax:Describe*",
        "dax:ListTags",
        "deepracer:ListModels",
        "detective:GetGraphIngestState",
        "detective:ListGraphs",
        "detective:ListMembers",
        "devicefarm:ListProjects",
        "directconnect:Describe*",
        "discovery:DescribeAgents",
        "discovery:DescribeConfigurations",
        "discovery:DescribeContinuousExports",
        "discovery:DescribeExportConfigurations",
        "discovery:DescribeExportTasks",
        "discovery:DescribeImportTasks",
        "dms:Describe*",
        "dms:ListTagsForResource",
        "docdb-elastic:ListClusters",
        "ds:DescribeDirectories",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeExport",
        "dynamodb:DescribeGlobalTable",
        "dynamodb:DescribeKinesisStreamingDestination",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:ListBackups",
        "dynamodb:ListExports",
        "dynamodb:ListGlobalTables",
        "dynamodb:ListStreams",
        "dynamodb:ListTables",
        "dynamodb:ListTagsOfResource",
        "ec2:Describe*",
        "ec2:GetAllowedImagesSettings",
        "ec2:GetEbsDefaultKmsKeyId",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetImageBlockPublicAccessState",
        "ec2:GetInstanceMetadataDefaults",
        "ec2:GetManagedPrefixListAssociations",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetNetworkInsightsAccessScopeAnalysisFindings",
        "ec2:GetNetworkInsightsAccessScopeContent",
        "ec2:GetSerialConsoleAccessStatus",
        "ec2:GetSnapshotBlockPublicAccessState",
```

```
        "ec2:GetTransitGatewayAttachmentPropagations",
        "ec2:GetTransitGatewayMulticastDomainAssociations",
        "ec2:GetTransitGatewayPrefixListReferences",
        "ec2:GetTransitGatewayPrefixListReferences",
        "ec2:GetTransitGatewayRouteTableAssociations",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:SearchTransitGatewayRoutes",
        "ec2:SearchTransitGatewayRoutes",
        "ecr-public:DescribeImages",
        "ecr-public:DescribeImageTags",
        "ecr-public:DescribeRegistries",
        "ecr-public:DescribeRepositories",
        "ecr-public:GetRegistryCatalogData",
        "ecr-public:GetRepositoryCatalogData",
        "ecr-public:GetRepositoryPolicy",
        "ecr-public:ListTagsForResource",
        "ecr:BatchGetRepositoryScanningConfiguration",
        "ecr:DescribeImages",
        "ecr:DescribeImageScanFindings",
        "ecr:DescribeRegistry",
        "ecr:DescribeRepositories",
        "ecr:GetLifecyclePolicy",
        "ecr:GetRegistryPolicy",
        "ecr:GetRegistryScanningConfiguration",
        "ecr:GetRepositoryPolicy",
        "ecr:ListImages",
        "ecr:ListTagsForResource",
        "ecs:Describe*",
        "ecs:List*",
        "eks:DescribeCluster",
        "eks:DescribeFargateProfile",
        "eks:DescribeNodeGroup",
        "eks:ListClusters",
        "eks:ListFargateProfiles",
        "eks:ListNodeGroups",
        "eks:ListTagsForResource",
        "eks:ListUpdates",
        "elasticache:Describe*",
        "elasticache:ListTagsForResource",
        "elasticbeanstalk:Describe*",
        "elasticbeanstalk:ListTagsForResource",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeAccountPreferences",
        "elasticfilesystem:DescribeBackupPolicy",
```

```
        "elasticfilesystem:DescribeFileSystemPolicy",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeMountTargetSecurityGroups",
        "elasticfilesystem:DescribeReplicationConfigurations",
        "elasticfilesystem:DescribeTags",
        "elasticloadbalancing:Describe*",
        "elasticmapreduce:Describe*",
        "elasticmapreduce:GetAutoTerminationPolicy",
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:GetManagedScalingPolicy",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListSecurityConfigurations",
        "elastictranscoder:ListPipelines",
        "emr-serverless:GetApplication",
        "emr-serverless:ListApplications",
        "emr-serverless:ListJobRuns",
        "entityresolution:GetIdNamespace",
        "es:Describe*",
        "es:GetCompatibleVersions",
        "es:ListDomainNames",
        "es:ListElasticsearchInstanceTypeDetails",
        "es:ListElasticsearchVersions",
        "es:ListTags",
        "events:Describe*",
        "events:List*",
        "events:TestEventPattern",
        "finspace:ListEnvironments",
        "finspace:ListKxEnvironments",
        "firehose:Describe*",
        "firehose:List*",
        "fms:ListComplianceStatus",
        "fms:ListPolicies",
        "forecast:ListDatasets",
        "frauddetector:GetDetectors",
        "fsx:Describe*",
        "fsx:List*",
        "gamelift:ListBuilds",
        "gamelift:ListFleets",
        "geo:ListMaps",
        "glacier:DescribeVault",
        "glacier:GetDataRetrievalPolicy",
```

```
        "glacier:GetVaultAccessPolicy",
        "glacier:GetVaultLock",
        "glacier:ListVaults",
        "globalaccelerator:Describe*",
        "globalaccelerator:List*",
        "glue:GetCrawlers",
        "glue:GetDatabases",
        "glue:GetDataCatalogEncryptionSettings",
        "glue:GetDevEndpoints",
        "glue:GetJobs",
        "glue:GetResourcePolicy",
        "glue:GetSecurityConfiguration",
        "glue:GetSecurityConfigurations",
        "glue:GetTags",
        "grafana:ListWorkspaces",
        "greengrass:List*",
        "guardduty:DescribePublishingDestination",
        "guardduty:DescribeOrganizationConfiguration",
        "guardduty:DescribeMalwareScans",
        "guardduty:Get*",
        "guardduty:List*",
        "health:DescribeAffectedAccountsForOrganization",
        "health:DescribeAffectedEntities",
        "health:DescribeAffectedEntitiesForOrganization",
        "health:DescribeEntityAggregates",
        "health:DescribeEventAggregates",
        "health:DescribeEventDetails",
        "health:DescribeEventDetailsForOrganization",
        "health:DescribeEvents",
        "health:DescribeEventsForOrganization",
        "health:DescribeEventTypes",
        "health:DescribeHealthServiceStatusForOrganization",
        "healthlake:ListFHIRDatastores",
        "honeycode:ListTables",
        "iam:GenerateCredentialReport",
        "iam:GenerateServiceLastAccessedDetails",
        "iam:Get*",
        "iam:List*",
        "iam:SimulateCustomPolicy",
        "iam:SimulatePrincipalPolicy",
        "identitystore:DescribeGroupMembership",
        "identitystore:GetGroupId",
        "identitystore:GetGroupMembershipId",
        "identitystore:GetUserId",
```

```
        "identitystore:IsMemberInGroups",
        "identitystore:ListGroupMemberships",
        "identitystore:ListGroupMembershipsForMember",
        "identitystore:ListGroups",
        "identitystore:ListUsers",
        "inspector:Describe*",
        "inspector:Get*",
        "inspector:List*",
        "inspector:Preview*",
        "inspector2:BatchGetAccountStatus",
        "inspector2:BatchGetFreeTrialInfo",
        "inspector2:DescribeOrganizationConfiguration",
        "inspector2:GetConfiguration",
        "inspector2:GetDelegatedAdminAccount",
        "inspector2:GetFindingsReportStatus",
        "inspector2:GetMember",
        "inspector2:ListAccountPermissions",
        "inspector2:ListCoverage",
        "inspector2:ListCoverageStatistics",
        "inspector2:ListDelegatedAdminAccounts",
        "inspector2:ListFilters",
        "inspector2:ListFindingAggregations",
        "inspector2:ListFindings",
        "inspector2:ListTagsForResource",
        "inspector2:ListUsageTotals",
        "iot:Describe*",
        "iot:GetPolicy",
        "iot:GetPolicyVersion",
        "iot:List*",
        "iotanalytics:ListChannels",
        "iotevents:ListInputs",
        "iotfleetwise:ListModelManifests",
        "iotsitewise:DescribeGatewayCapabilityConfiguration",
        "iotsitewise:ListAssetModels",
        "iotsitewise:ListGateways",
        "iottwinmaker:ListWorkspaces",
        "kafka-cluster:Describe*",
        "kafka:Describe*",
        "kafka:GetBootstrapBrokers",
        "kafka:GetCompatibleKafkaVersions",
        "kafka:List*",
        "kafkaconnect:Describe*",
        "kafkaconnect:List*",
        "kendra:DescribeIndex",
```

```
        "kendra:ListDataSources",
        "kendra:ListIndices",
        "kendra:ListTagsForResource",
        "kinesis:DescribeLimits",
        "kinesis:DescribeStream",
        "kinesis:DescribeStreamConsumer",
        "kinesis:DescribeStreamSummary",
        "kinesis:ListShards",
        "kinesis:ListStreamConsumers",
        "kinesis:ListStreams",
        "kinesis:ListTagsForStream",
        "kinesisanalytics:ListApplications",
        "kinesisanalytics:ListTagsForResource",
        "kinesisvideo:DescribeEdgeConfiguration",
        "kinesisvideo:DescribeMappedResourceConfiguration",
        "kinesisvideo:DescribeMediaStorageConfiguration",
        "kinesisvideo:DescribeNotificationConfiguration",
        "kinesisvideo:DescribeSignalingChannel",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:ListSignalingChannels",
        "kinesisvideo:ListStreams",
        "kinesisvideo:ListTagsForResource",
        "kinesisvideo:ListTagsForStream",
        "kms:Describe*",
        "kms:Get*",
        "kms:List*",
        "lambda:GetAccountSettings",
        "lambda:GetFunctionConfiguration",
        "lambda:GetFunctionEventInvokeConfig",
        "lambda:GetLayerVersionPolicy",
        "lambda:GetPolicy",
        "lambda:List*",
        "lex:DescribeBot",
        "lex:DescribeResourcePolicy",
        "lex:ListBots",
        "license-manager:List*",
        "lightsail:GetBuckets",
        "lightsail:GetContainerServices",
        "lightsail:GetDisks",
        "lightsail:GetDiskSnapshots",
        "lightsail:GetInstances",
        "lightsail:GetLoadBalancers",
        "logs:Describe*",
        "logs:GetLogDelivery",
```

```
        "logs:ListLogDeliveries",
        "logs:ListTagsForResource",
        "logs:ListTagsLogGroup",
        "lookoutequipment:ListDatasets",
        "lookoutmetrics:ListAnomalyDetectors",
        "lookoutvision:ListProjects",
        "m2:GetApplication",
        "m2:GetEnvironment",
        "m2:ListApplications",
        "m2:ListEnvironments",
        "m2:ListTagsForResource",
        "machinelearning:DescribeMLModels",
        "macie2:ListFindings",
        "managedblockchain:ListNetworks",
        "mechanicalturk:ListHITs",
        "mediaconnect:Describe*",
        "mediaconnect:List*",
        "medialive:ListChannels",
        "mediapackage-vod:DescribePackagingGroup",
        "mediapackage-vod:ListPackagingGroups",
        "mediapackage:DescribeOriginEndpoint",
        "mediapackage:ListOriginEndpoints",
        "mediastore:GetContainerPolicy",
        "mediastore:GetCorsPolicy",
        "mediastore:ListContainers",
        "memorydb:DescribeClusters",
        "mq:DescribeBroker",
        "mq:DescribeBrokerEngineTypes",
        "mq:DescribeBrokerInstanceOptions",
        "mq:DescribeConfiguration",
        "mq:DescribeConfigurationRevision",
        "mq:DescribeUser",
        "mq:ListBrokers",
        "mq:ListConfigurationRevisions",
        "mq:ListConfigurations",
        "mq:ListTags",
        "mq:ListUsers",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeLoggingConfiguration",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
```

```
        "network-firewall:ListRuleGroups",
        "networkmanager:DescribeGlobalNetworks",
        "nimble:ListStudios",
        "opsworks-cm:DescribeServers",
        "opsworks:DescribeStacks",
        "organizations:Describe*",
        "organizations:List*",
        "pcs:GetCluster",
        "pcs:GetComputeNodeGroup",
        "pcs:GetQueue",
        "pcs:ListClusters",
        "pcs:ListComputeNodeGroups",
        "pcs:ListQueues",
        "pcs:ListTagsForResource",
        "personalize:DescribeDatasetGroup",
        "personalize:ListDatasetGroups",
        "private-networks:ListNetworks",
        "profile:GetDomain",
        "profile:ListDomains",
        "profile:ListIntegrations",
        "qbusiness:ListApplications",
        "qbusiness:ListDataSources",
        "qbusiness:ListDataSourceSyncJobs",
        "qbusiness:ListDocuments",
        "qbusiness:ListGroups",
        "qbusiness:ListIndices",
        "qbusiness:ListPlugins",
        "qbusiness:ListRetrievers",
        "qbusiness:ListSubscriptions",
        "qbusiness:ListTagsForResource",
        "qbusiness:ListWebExperiences",
        "qldb:DescribeJournalS3Export",
        "qldb:DescribeLedger",
        "qldb:ListJournalS3Exports",
        "qldb:ListJournalS3ExportsForLedger",
        "qldb:ListLedgers",
        "quicksight:Describe*",
        "quicksight:List*",
        "ram:GetResourceShares",
        "ram:List*",
        "rds:Describe*",
        "rds:DownloadDBLogFilePortion",
        "rds:ListTagsForResource",
        "redshift-serverless:GetNamespace",
```

```
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:ListWorkgroups",
        "redshift:Describe*",
        "rekognition:Describe*",
        "rekognition:List*",
        "resource-groups:ListGroupResources",
        "robomaker:Describe*",
        "robomaker:List*",
        "rolesanywhere:GetCrl",
        "rolesanywhere:GetProfile",
        "rolesanywhere:GetSubject",
        "rolesanywhere:GetTrustAnchor",
        "rolesanywhere:ListCrls",
        "rolesanywhere:ListProfiles",
        "rolesanywhere:ListSubjects",
        "rolesanywhere:ListTagsForResource",
        "rolesanywhere:ListTrustAnchors",
        "route53:Get*",
        "route53:List*",
        "route53domains:GetDomainDetail",
        "route53domains:GetOperationDetail",
        "route53domains:ListDomains",
        "route53domains:ListOperations",
        "route53domains:ListTagsForDomain",
        "route53resolver:Get*",
        "route53resolver:List*",
        "s3-outposts:ListEndpoints",
        "s3-outposts:ListOutpostsWithS3",
        "s3-outposts:ListSharedEndpoints",
        "s3:DescribeJob",
        "s3:GetAccelerateConfiguration",
        "s3:GetAccessGrantsInstanceResourcePolicy",
        "s3:GetAccessPoint",
        "s3:GetAccessPointConfigurationForObjectLambda",
        "s3:GetAccessPointPolicy",
        "s3:GetAccessPointPolicyForObjectLambda",
        "s3:GetAccessPointPolicyStatus",
        "s3:GetAccessPointPolicyStatusForObjectLambda",
        "s3:GetAccessPointForObjectLambda",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetAnalyticsConfiguration",
        "s3:GetBucket*",
        "s3:GetEncryptionConfiguration",
        "s3:GetInventoryConfiguration",
```

```
        "s3:GetLifecycleConfiguration",
        "s3:GetMetricsConfiguration",
        "s3:GetMultiRegionAccessPoint",
        "s3:GetMultiRegionAccessPointPolicy",
        "s3:GetMultiRegionAccessPointPolicyStatus",
        "s3:GetObjectAcl",
        "s3:GetObjectTagging",
        "s3:GetObjectVersionAcl",
        "s3:GetReplicationConfiguration",
        "s3:GetStorageLensGroup",
        "s3:GetStorageLensConfiguration",
        "s3:ListAccessPoints",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListMultiRegionAccessPoints",
        "s3:ListAccessPointsForObjectLambda",
        "s3:ListStorageLensGroups",
        "s3:ListJobs",
        "s3:ListCallerAccessGrants",
        "s3:ListAccessGrantsInstances",
        "s3:ListAccessGrants",
        "s3:ListStorageLensConfigurations",
        "s3express:ListAllMyDirectoryBuckets",
        "s3express:GetEncryptionConfiguration",
        "s3express:GetBucketPolicy",
        "s3-object-lambda:GetObjectAcl",
        "s3-object-lambda:GetObjectVersionAcl",
        "s3tables:ListTableBuckets",
        "s3tables:ListNamespaces",
        "s3tables:ListTables",
        "s3tables:GetNamespace",
        "s3tables:GetTableBucketPolicy",
        "s3tables:GetTableBucketMaintenanceConfiguration",
        "s3tables:GetTableMaintenanceConfiguration",
        "s3tables:GetTablePolicy",
        "sagemaker:Describe*",
        "sagemaker:List*",
        "schemas:DescribeCodeBinding",
        "schemas:DescribeDiscoverer",
        "schemas:DescribeRegistry",
        "schemas:DescribeSchema",
        "schemas:GetResourcePolicy",
        "schemas:ListDiscoverers",
        "schemas:ListRegistries",
```

```
        "schemas:ListSchemas",
        "schemas:ListSchemaVersions",
        "schemas:ListTagsForResource",
        "sdb:DomainMetadata",
        "sdb:ListDomains",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:ListSecrets",
        "secretsmanager:ListSecretVersionIds",
        "securityhub:BatchGetAutomationRules",
        "securityhub:BatchGetConfigurationPolicyAssociations",
        "securityhub:BatchGetControlEvaluations",
        "securityhub:BatchGetSecurityControls",
        "securityhub:BatchGetStandardsControlAssociations",
        "securityhub:Describe*",
        "securityhub:Get*",
        "securityhub:List*",
        "serverlessrepo:GetApplicationPolicy",
        "serverlessrepo:List*",
        "servicequotas:GetAssociationForServiceQuotaTemplate",
        "servicequotas:GetAWSDefaultServiceQuota",
        "servicequotas:GetRequestedServiceQuotaChange",
        "servicequotas:GetServiceQuota",
        "servicequotas:GetServiceQuotaIncreaseRequestFromTemplate",
        "servicequotas:ListAWSDefaultServiceQuotas",
        "servicequotas:ListRequestedServiceQuotaChangeHistory",
        "servicequotas:ListRequestedServiceQuotaChangeHistoryByQuota",
        "servicequotas:ListServiceQuotaIncreaseRequestsInTemplate",
        "servicequotas:ListServiceQuotas",
        "servicequotas:ListServices",
        "servicequotas:ListTagsForResource",
        "ses:Describe*",
        "ses:GetAccount",
        "ses:GetAccountSendingEnabled",
        "ses:GetConfigurationSet",
        "ses:GetConfigurationSetEventDestinations",
        "ses:GetDedicatedIps",
        "ses:GetEmailIdentity",
        "ses:GetIdentityDkimAttributes",
        "ses:GetIdentityPolicies",
        "ses:GetIdentityVerificationAttributes",
        "ses:ListConfigurationSets",
        "ses:ListDedicatedIpPools",
        "ses:ListIdentities",
```

```
        "ses:ListIdentityPolicies",
        "ses:ListReceiptFilters",
        "ses:ListReceiptRuleSets",
        "ses:ListVerifiedEmailAddresses",
        "shield:Describe*",
        "shield:GetSubscriptionState",
        "shield:List*",
        "snowball:ListClusters",
        "snowball:ListJobs",
        "sns:GetPlatformApplicationAttributes",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTagsForResource",
        "sns:ListTopics",
        "sqs:GetQueueAttributes",
        "sqs:ListDeadLetterSourceQueues",
        "sqs:ListQueues",
        "sqs:ListQueueTags",
        "ssm:Describe*",
        "ssm:GetAutomationExecution",
        "ssm:GetServiceSetting",
        "ssm:ListAssociations",
        "ssm:ListAssociationVersions",
        "ssm:ListCommands",
        "ssm:ListComplianceItems",
        "ssm:ListComplianceSummaries",
        "ssm:ListDocumentMetadataHistory",
        "ssm:ListDocuments",
        "ssm:ListDocumentVersions",
        "ssm:ListInventoryEntries",
        "ssm:ListOpsMetadata",
        "ssm:ListResourceComplianceSummaries",
        "ssm:ListResourceDataSync",
        "ssm:ListTagsForResource",
        "sso:DescribeAccountAssignmentCreationStatus",
        "sso:DescribePermissionSet",
        "sso:DescribeAccountAssignmentDeletionStatus",
        "sso:DescribeApplication",
        "sso:DescribeApplicationAssignment",
        "sso:DescribeApplicationProvider",
        "sso:DescribeInstance",
        "sso:DescribeInstanceAccessControlAttributeConfiguration",
        "sso:DescribePermissionSetProvisioningStatus",
```

```
        "sso:DescribeTrustedTokenIssuer",
        "sso:GetApplicationAccessScope",
        "sso:GetApplicationAssignmentConfiguration",
        "sso:GetApplicationAuthenticationMethod",
        "sso:GetApplicationGrant",
        "sso:GetInlinePolicyForPermissionSet",
        "sso:GetPermissionsBoundaryForPermissionSet",
        "sso:ListAccountAssignmentCreationStatus",
        "sso:ListAccountAssignmentDeletionStatus",
        "sso:ListAccountAssignments",
        "sso:ListAccountAssignmentsForPrincipal",
        "sso:ListAccountsForProvisionedPermissionSet",
        "sso:ListApplicationAccessScopes",
        "sso:ListApplicationAssignments",
        "sso:ListApplicationAssignmentsForPrincipal",
        "sso:ListApplicationAuthenticationMethods",
        "sso:ListApplicationGrants",
        "sso:ListApplicationInstanceCertificates",
        "sso:ListApplicationInstances",
        "sso:ListApplicationProviders",
        "sso:ListApplications",
        "sso:ListApplicationTemplates",
        "sso:ListCustomerManagedPolicyReferencesInPermissionSet",
        "sso:ListDirectoryAssociations",
        "sso:ListInstances",
        "sso:ListManagedPoliciesInPermissionSet",
        "sso:ListPermissionSetProvisioningStatus",
        "sso:ListPermissionSets",
        "sso:ListPermissionSetsProvisionedToAccount",
        "sso:ListProfileAssociations",
        "sso:ListProfiles",
        "sso:ListTagsForResource",
        "sso:ListTrustedTokenIssuers",
        "states:DescribeStateMachine",
        "states:ListStateMachines",
        "storagegateway:DescribeBandwidthRateLimit",
        "storagegateway:DescribeCache",
        "storagegateway:DescribeCachediSCSIVolumes",
        "storagegateway:DescribeGatewayInformation",
        "storagegateway:DescribeMaintenanceStartTime",
        "storagegateway:DescribeNFSFileShares",
        "storagegateway:DescribeSnapshotSchedule",
        "storagegateway:DescribeStorediSCSIVolumes",
        "storagegateway:DescribeTapeArchives",
```

```
        "storagegateway:DescribeTapeRecoveryPoints",
        "storagegateway:DescribeTapes",
        "storagegateway:DescribeUploadBuffer",
        "storagegateway:DescribeVTLDevices",
        "storagegateway:DescribeWorkingStorage",
        "storagegateway:List*",
        "sts:GetAccessKeyInfo",
        "support:DescribeTrustedAdvisorCheckRefreshStatuses",
        "support:DescribeTrustedAdvisorCheckResult",
        "support:DescribeTrustedAdvisorChecks",
        "support:DescribeTrustedAdvisorCheckSummaries",
        "synthetics:DescribeCanaries",
        "synthetics:DescribeCanariesLastRun",
        "synthetics:DescribeRuntimeVersions",
        "synthetics:GetCanary",
        "synthetics:GetCanaryRuns",
        "synthetics:GetGroup",
        "synthetics:ListAssociatedGroups",
        "synthetics:ListGroupResources",
        "synthetics:ListGroups",
        "synthetics:ListTagsForResource",
        "tag:GetResources",
        "tag:GetTagKeys",
        "transcribe:GetCallAnalyticsCategory",
        "transcribe:GetMedicalVocabulary",
        "transcribe:GetVocabulary",
        "transcribe:GetVocabularyFilter",
        "transcribe:ListCallAnalyticsCategories",
        "transcribe:ListCallAnalyticsJobs",
        "transcribe:ListLanguageModels",
        "transcribe:ListMedicalTranscriptionJobs",
        "transcribe:ListMedicalVocabularies",
        "transcribe:ListTagsForResource",
        "transcribe:ListTranscriptionJobs",
        "transcribe:ListVocabularies",
        "transcribe:ListVocabularyFilters",
        "transfer:Describe*",
        "transfer:List*",
        "translate:List*",
        "trustedadvisor:Describe*",
        "voiceid:DescribeDomain",
        "waf-regional:GetWebACL",
        "waf-regional:ListResourcesForWebACL",
        "waf-regional:ListTagsForResource",
```

```
        "waf-regional:ListWebACLs",
        "waf:GetWebACL",
        "waf:ListTagsForResource",
        "waf:ListWebACLs",
        "wafv2:GetLoggingConfiguration",
        "wafv2:GetWebACL",
        "wafv2:GetWebACLForResource",
        "wafv2:ListAvailableManagedRuleGroups",
        "wafv2:ListIPSets",
        "wafv2:ListLoggingConfigurations",
        "wafv2:ListRegexPatternSets",
        "wafv2:ListResourcesForWebACL",
        "wafv2:ListRuleGroups",
        "wafv2:ListTagsForResource",
        "wafv2:ListWebACLs",
        "wisdom:GetAssistant",
        "workdocs:DescribeResourcePermissions",
        "workspaces:Describe*",
        "xray:GetEncryptionConfig",
        "xray:GetGroup",
        "xray:GetGroups",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetTraceSummaries",
        "xray:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "APIGatewayAccess",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*/authorizers/*",
        "arn:aws:apigateway:*::/apis/*/authorizers",
        "arn:aws:apigateway:*::/apis/*/cors",
        "arn:aws:apigateway:*::/apis/*/deployments/*",
        "arn:aws:apigateway:*::/apis/*/deployments",
        "arn:aws:apigateway:*::/apis/*/exports/*",
        "arn:aws:apigateway:*::/apis/*/integrations/*",
        "arn:aws:apigateway:*::/apis/*/integrations",
```

```
        "arn:aws:apigateway:*::/apis/*/models/*",
        "arn:aws:apigateway:*::/apis/*/models",
        "arn:aws:apigateway:*::/apis/*/routes/*",
        "arn:aws:apigateway:*::/apis/*/routes",
        "arn:aws:apigateway:*::/apis/*/stages",
        "arn:aws:apigateway:*::/apis/*/stages/*",
        "arn:aws:apigateway:*::/clientcertificates",
        "arn:aws:apigateway:*::/clientcertificates/*",
        "arn:aws:apigateway:*::/domainnames",
        "arn:aws:apigateway:*::/domainnames/*/apimappings",
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*/authorizers/*",
        "arn:aws:apigateway:*::/restapis/*/authorizers",
        "arn:aws:apigateway:*::/restapis/*/deployments/*",
        "arn:aws:apigateway:*::/restapis/*/deployments",
        "arn:aws:apigateway:*::/restapis/*/documentation/parts/*",
        "arn:aws:apigateway:*::/restapis/*/documentation/parts",
        "arn:aws:apigateway:*::/restapis/*/documentation/versions/*",
        "arn:aws:apigateway:*::/restapis/*/documentation/versions",
        "arn:aws:apigateway:*::/restapis/*/gatewayresponses/*",
        "arn:aws:apigateway:*::/restapis/*/gatewayresponses",
        "arn:aws:apigateway:*::/restapis/*/models/*",
        "arn:aws:apigateway:*::/restapis/*/models",
        "arn:aws:apigateway:*::/restapis/*/requestvalidators",
        "arn:aws:apigateway:*::/restapis/*/requestvalidators/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*",
        "arn:aws:apigateway:*::/restapis/*/resources",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/tags/*",
        "arn:aws:apigateway:*::/vpclinks"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

SecurityLakeResourceManagementServiceRolePolicy

説明: Security Lake が作成したリソースを管理するためのアクセスを提供します。

SecurityLakeResourceManagementServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2024 年 11 月 14 日 22:10 UTC
- 編集日時: 2025 年 11 月 19 日 18:49 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/SecurityLakeResourceManagementServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadEventBridgeRules",
      "Effect" : "Allow",
      "Action" : [
        "events:ListRules"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ManageSecurityLakeEventRules",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/AmazonSecurityLake-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ManageSecurityLakeLambdaConfigurations",
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetEventSourceMapping",
        "lambda:GetFunction",
        "lambda:PutFunctionConcurrency",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:GetFunctionConcurrency",
        "lambda:GetRuntimeManagementConfig",
        "lambda:PutProvisionedConcurrencyConfig",
        "lambda:PublishVersion",
        "lambda:DeleteFunctionConcurrency",
        "lambda:DeleteEventSourceMapping",
        "lambda:GetAlias",
        "lambda:GetPolicy",
        "lambda:GetFunctionConfiguration",
        "lambda:UpdateFunctionConfiguration"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*",
        "arn:aws:lambda:*:*:function:AmazonSecurityLakeMetastoreManager-*-*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DeletePartitionUpdaterLambda",
      "Effect" : "Allow",
      "Action" : "lambda:DeleteFunction",
      "Resource" :
"arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowListLambdaEventSourceMappings",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListEventSourceMappings"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowUpdateLambdaEventSourceMapping",
      "Effect" : "Allow",
      "Action" : [
        "lambda:UpdateEventSourceMapping"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ArnLike" : {
          "lambda:FunctionArn" :
"arn:aws:lambda:*:*:function:AmazonSecurityLakeMetastoreManager-*-*"
        }
```

```
      }
    },
    {
      "Sid" : "AllowUpdateLambdaConfigs",
      "Effect" : "Allow",
      "Action" : [
        "lambda:UpdateFunctionConfiguration"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:AmazonSecurityLakeMetastoreManager-*-
*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ManageSecurityLakeGlueResources",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreatePartition",
        "glue:BatchCreatePartition",
        "glue:GetTable",
        "glue:GetTables",
        "glue:UpdateTable",
        "glue:GetDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/amazon_security_lake_glue_db*/*",
        "arn:aws:glue:*:*:database/amazon_security_lake_glue_db*",
        "arn:aws:glue:*:*:catalog"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowDataLakeConfigurationManagement",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:PutObject",
```

```
        "s3:GetObjectAttributes",
        "s3:GetBucketNotification",
        "s3:PutBucketNotification",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:GetEncryptionConfiguration",
        "s3:GetReplicationConfiguration"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-security-data-lake*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowMetaDataCompactionAndManagement",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:DeleteObject",
        "s3:RestoreObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-security-data-lake*/metadata/*.avro",
        "arn:aws:s3:::aws-security-data-lake*/metadata/*.metadata.json"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ReadSecurityLakeLambdaLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:StartQuery",
        "logs:GetLogEvents",
        "logs:GetQueryResults",
        "logs:GetLogRecord"
```

```
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/lambda/AmazonSecurityLakeMetastoreManager-*-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ManageSecurityLakeSQSQueue",
      "Effect" : "Allow",
      "Action" : [
        "sqs:StartMessageMoveTask",
        "sqs:DeleteMessage",
        "sqs:GetQueueUrl",
        "sqs:ListDeadLetterSourceQueues",
        "sqs:ChangeMessageVisibility",
        "sqs:ListMessageMoveTasks",
        "sqs:ReceiveMessage",
        "sqs:SendMessage",
        "sqs:GetQueueAttributes",
        "sqs:SetQueueAttributes"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:SecurityLake_*",
        "arn:aws:sqs:*:*:AmazonSecurityLakeManager-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowDataLakeManagement",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataLakeSettings",
        "lakeformation:ListPermissions"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

SecurityLakeServiceLinkedRole

説明: このポリシーでは、ユーザー代わって Amazon Security Lake サービスを運用する許可が付与されます。

SecurityLakeServiceLinkedRole は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 11 月 29 日 14:03 UTC
- 編集日時: 2024 年 4 月 19 日 16:00 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/SecurityLakeServiceLinkedRole

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

ServerMigration_ServiceRole

説明: AWS Server Migration Service が VMs を EC2 に移行できるようにするアクセス許可: Server Migration Service が移行したリソースを顧客の EC2 アカウントに配置することを許可します。

`ServerMigration_ServiceRole` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `ServerMigration_ServiceRole` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 8 月 11 日 20:41 UTC
- 編集日時: 2020 年 10 月 15 日 17:26 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ServerMigration_ServiceRole`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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-*/*"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

ServerMigrationConnector

説明: AWS Server Migration Connector が VMs を EC2 に移行できるようにするアクセス許可。AWS Server Migration Service との通信、'sms-b-' および 'import-to-ec2-' で始まる S3 バケットへの読み取り/書き込みアクセス、および AWS Server Migration Connector のアップグレード、 AWS Server Migration Connector への登録 AWS、メトリクスのアップロードに使用されるバケットを許可します AWS。

`ServerMigrationConnector` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `ServerMigrationConnector` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2016 年 10 月 24 日 21:45 UTC
- 編集日時: 2016 年 10 月 24 日 21:45 UTC
- ARN: `arn:aws:iam::aws:policy/ServerMigrationConnector`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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-*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

ServerMigrationServiceConsoleFullAccess

説明: Server Migration Service Console のすべての機能を使用するために必要な許可

`ServerMigrationServiceConsoleFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `ServerMigrationServiceConsoleFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 5 月 9 日 17:18 UTC
- 編集日時: 2020 年 7 月 20 日 22:00 UTC
- ARN: `arn:aws:iam::aws:policy/ServerMigrationServiceConsoleFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

ServerMigrationServiceLaunchRole

説明: AWS Server Migration Service が、移行されたサーバーとアプリケーションを起動 AWS アカウント するための関連 AWS リソースを作成してお客様の に更新できるようにするアクセス許可。

`ServerMigrationServiceLaunchRole` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `ServerMigrationServiceLaunchRole` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2018 年 11 月 26 日 19:53 UTC
- 編集日時: 2020 年 10 月 15 日 17:29 UTC

- ARN: arn:aws:iam::aws:policy/service-role/ServerMigrationServiceLaunchRole

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

ServerMigrationServiceRoleForInstanceValidation

説明: SMS AWS が使用済みデータ検証スクリプトを実行し、スクリプトの成功/失敗を SMS に送信できるようにするアクセス許可

`ServerMigrationServiceRoleForInstanceValidation` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `ServerMigrationServiceRoleForInstanceValidation` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 7 月 20 日 22:25 UTC
- 編集日時: 2020 年 7 月 20 日 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ServerMigrationServiceRoleForInstanceValidation`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::sms-app-*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "sms:NotifyAppValidationOutput",
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

ServiceQuotasFullAccess

説明: Service Quotas へのフルアクセスを提供します

`ServiceQuotasFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `ServiceQuotasFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 6 月 24 日 15:44 UTC

- 編集日時: 2021 年 2 月 4 日 21:29 UTC
- ARN: arn:aws:iam::aws:policy/ServiceQuotasFullAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する

- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

ServiceQuotasReadOnlyAccess

説明: Service Quotas への読み取り専用アクセスを提供します

`ServiceQuotasReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `ServiceQuotasReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 6 月 24 日 15:31 UTC
- 編集日時: 2025 年 10 月 13 日 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/ServiceQuotasReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAccountLimits",
```

```
        "cloudformation:DescribeAccountLimits",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "dynamodb:DescribeLimits",
        "elasticloadbalancing:DescribeAccountLimits",
        "iam:GetAccountSummary",
        "kinesis:DescribeLimits",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "rds:DescribeAccountAttributes",
        "route53:GetAccountLimit",
        "tag:GetTagKeys",
        "tag:GetTagValues",
        "servicequotas:GetAssociationForServiceQuotaTemplate",
        "servicequotas:GetAWSDefaultServiceQuota",
        "servicequotas:GetRequestedServiceQuotaChange",
        "servicequotas:GetServiceQuota",
        "servicequotas:GetServiceQuotaIncreaseRequestFromTemplate",
        "servicequotas:ListAWSDefaultServiceQuotas",
        "servicequotas:ListRequestedServiceQuotaChangeHistory",
        "servicequotas:ListRequestedServiceQuotaChangeHistoryByQuota",
        "servicequotas:ListServices",
        "servicequotas:ListServiceQuotas",
        "servicequotas:ListServiceQuotaIncreaseRequestsInTemplate",
        "servicequotas:ListTagsForResource",
        "servicequotas:GetAutoManagementConfiguration",
        "notifications:ListChannels",
        "notifications:ListEventRules",
        "notifications:ListNotificationConfigurations",
        "notifications:GetNotificationConfiguration",
        "notifications:GetEventRule",
        "notifications:ListNotificationHubs",
        "notifications-contacts:ListEmailContacts",
        "notifications-contacts:GetEmailContact",
        "chatbot:ListMicrosoftTeamsChannelConfigurations",
        "chatbot:DescribeChimeWebhookConfigurations",
        "chatbot:DescribeSlackChannelConfigurations",
        "consoleapp:ListDeviceIdentities",
        "consoleapp:GetDeviceIdentity"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

ServiceQuotasServiceRolePolicy

説明: Service Quotas に、お客様のためにサポートケースを作成する許可を付与します

`ServiceQuotasServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 5 月 22 日 20:44 UTC
- 編集日時: 2019 年 6 月 24 日 14:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ServiceQuotasServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "support:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

SignInLocalDevelopmentAccess

説明: 開発者ツールとアプリケーションの OAuth2 トークンの作成など、 AWS サインインサービス AWS を通じて にプログラムでアクセスするためのアクセス許可を提供します。

`SignInLocalDevelopmentAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `SignInLocalDevelopmentAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2025 年 11 月 19 日 18:34 UTC

- 編集日時: 2025 年 11 月 19 日 18:34 UTC
- ARN: `arn:aws:iam::aws:policy/SignInLocalDevelopmentAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "signin:AuthorizeOAuth2Access",
        "signin:CreateOAuth2Token"
      ],
      "Resource" : "arn:aws:signin:*:*:oauth2/public-client/*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

SimpleWorkflowFullAccess

説明: Simple Workflow 設定サービスへのフルアクセスを提供します。

SimpleWorkflowFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに SimpleWorkflowFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2015 年 2 月 6 日 18:41 UTC
- ARN: arn:aws:iam::aws:policy/SimpleWorkflowFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "swf:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する

- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

SMSVoiceServiceRolePolicy

説明: SMSVoice がユーザーに代わって CloudWatch にメトリクスを発行できるようにします

SMSVoiceServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2024 年 11 月 14 日 17:04 UTC
- 編集日時: 2024 年 11 月 14 日 17:04 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/SMSVoiceServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/SMSVoice"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

SplitCostAllocationDataServiceRolePolicy

説明: 該当する場合は、分割コスト配分データで AWS Organizations 情報を取得し、顧客がオプトインした分割コスト配分データサービスのテレメトリデータを収集できるようにします。

`SplitCostAllocationDataServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2024 年 4 月 16 日 16:05 UTC
- 編集日時: 2024 年 4 月 16 日 16:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/SplitCostAllocationDataServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

SSMQuickSetupRolePolicy

説明: Quick Setup 設定の正常性をチェックし、パラメータおよびプロビジョニングされたリソースが一貫して使用されるよう保証するとともに、ドリフトが検出された際にリソースを修復する権限を付与します。

SSMQuickSetupRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2024 年 6 月 25 日 15:20 UTC
- 編集日時: 2024 年 11 月 18 日 13:06 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/SSMQuickSetupRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SSMResourceDataSyncPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListResourceDataSync"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMResourceDataSyncGetOpsSummaryPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetOpsSummary"
      ],
      "Resource" : "arn:aws:ssm:*:*:resource-data-sync/AWS-QuickSetup-*"
    },
    {
      "Sid" : "SSMResourceDataSyncManagePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteResourceDataSync"
      ],
      "Resource" : "arn:aws:ssm:*:*:resource-data-sync/AWS-QuickSetup-*",
      "Condition" : {
        "StringEquals" : {
          "ssm:SyncType" : "SyncFromSource"
        }
      }
    },
    {
      "Sid" : "SSMAssociationsReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListAssociations",
        "ssm:DescribeAssociationExecutions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "QuickSetupSSMDocumentsReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument",
        "ssm:GetDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSQuickSetupType-*",
        "arn:aws:ssm:*:*:document/*-AWSQuickSetupType-*"
      ]
```

```
    },
    {
      "Sid" : "OrganizationReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:ListRoots",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAccountsForParent",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListDelegatedServicesForAccount"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "QuickSetupStackSetReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:ListStackInstances",
        "cloudformation:ListStackSetOperations",
        "cloudformation:ListStackSetOperationResults",
        "cloudformation:GetTemplate"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stackset/AWS-QuickSetup-*",
        "arn:aws:cloudformation:*:*:stackset/SSMQuickSetup*",
        "arn:aws:cloudformation:*:*:stack/StackSet-AWS-QuickSetup-*",
        "arn:aws:cloudformation:*:*:stack/StackSet-SSMQuickSetup*"
      ]
    },
    {
      "Sid" : "QuickSetupStackSetDeletePermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DeleteStackInstances",
        "cloudformation:DeleteStackSet"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stackset/AWS-QuickSetup-*",
        "arn:aws:cloudformation:*:*:stackset/SSMQuickSetup*",
```

```
        "arn:aws:cloudformation:*:*:stack/StackSet-AWS-QuickSetup-*",
        "arn:aws:cloudformation:*:*:stack/StackSet-SSMQuickSetup*",
        "arn:aws:cloudformation:*:*:stackset-target/AWS-QuickSetup-*",
        "arn:aws:cloudformation:*:*:stackset-target/SSMQuickSetup*",
        "arn:aws:cloudformation:*:*:type/resource/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "QuickSetupCfnStacksDescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

SupportUser

説明: このポリシーは、 AWS アカウントの問題のトラブルシューティングおよび解決を行う許可を付与します。このポリシーにより、ユーザーは AWS サポートに連絡してケースを作成および管理することもできます。

SupportUser は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに SupportUser をアタッチできます。

ポリシーの詳細

- タイプ: ジョブ機能ポリシー
- 作成日時: 2016 年 11 月 10 日 17:21 UTC
- 編集日時: 2025 年 7 月 10 日 17:07 UTC
- ARN: arn:aws:iam::aws:policy/job-function/SupportUser

ポリシーのバージョン

ポリシーのバージョン: v9 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "support:*",
        "acm:DescribeCertificate",
        "acm:GetCertificate",
        "acm:List*",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:ListCertificateAuthorities",
        "apigateway:GET",
        "autoscaling:Describe*",
        "aws-marketplace:ViewSubscriptions",
        "cloudformation:Describe*",
        "cloudformation:Get*",
        "cloudformation:List*",
        "cloudformation:EstimateTemplateCost",
        "cloudfront:Get*",
```

```
        "cloudfront:List*",
        "cloudsearch:Describe*",
        "cloudsearch:List*",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:LookupEvents",
        "cloudtrail:ListTags",
        "cloudtrail:ListPublicKeys",
        "cloudwatch:Describe*",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "codecommit:BatchGetRepositories",
        "codecommit:Get*",
        "codecommit:List*",
        "codedeploy:Batch*",
        "codedeploy:Get*",
        "codedeploy:List*",
        "codepipeline:AcknowledgeJob",
        "codepipeline:AcknowledgeThirdPartyJob",
        "codepipeline:ListActionTypes",
        "codepipeline:ListPipelines",
        "codepipeline:PollForJobs",
        "codepipeline:PollForThirdPartyJobs",
        "codepipeline:GetPipelineState",
        "codepipeline:GetPipeline",
        "cognito-identity:List*",
        "cognito-identity:LookupDeveloperIdentity",
        "cognito-identity:Describe*",
        "cognito-idp:DescribeResourceServer",
        "cognito-idp:DescribeRiskConfiguration",
        "cognito-idp:DescribeUserImportJob",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolDomain",
        "cognito-idp:List*",
        "cognito-sync:Describe*",
        "cognito-sync:GetBulkPublishDetails",
        "cognito-sync:GetCognitoEvents",
        "cognito-sync:GetIdentityPoolConfiguration",
        "cognito-sync:List*",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:DescribeConfigRuleEvaluationStatus",
        "config:DescribeConfigRules",
        "config:DescribeDeliveryChannels",
```

```
        "config:DescribeDeliveryChannelStatus",
        "config:GetResourceConfigHistory",
        "config:ListDiscoveredResources",
        "datapipeline:DescribeObjects",
        "datapipeline:DescribePipelines",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:ListPipelines",
        "datapipeline:QueryObjects",
        "datapipeline:ReportTaskProgress",
        "datapipeline:ReportTaskRunnerHeartbeat",
        "devicefarm:List*",
        "devicefarm:Get*",
        "directconnect:Describe*",
        "discovery:Describe*",
        "discovery:ListConfigurations",
        "dms:Describe*",
        "dms:List*",
        "ds:DescribeDirectories",
        "ds:DescribeSnapshots",
        "ds:GetDirectoryLimits",
        "ds:GetSnapshotLimits",
        "ds:ListAuthorizedApplications",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeTable",
        "dynamodb:ListTables",
        "ec2:Describe*",
        "ec2:DescribeHosts",
        "ec2:describeIdentityIdFormat",
        "ec2:DescribeIdFormat",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeNatGateways",
        "ec2:DescribeReservedInstancesModifications",
        "ec2:DescribeTags",
        "ec2:SearchLocalGatewayRoutes",
        "ecr:GetRepositoryPolicy",
        "ecr:BatchCheckLayerAvailability",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "ecs:Describe*",
        "ecs:List*",
        "elasticache:Describe*",
        "elasticache:List*",
        "elasticbeanstalk:Check*",
        "elasticbeanstalk:Describe*",
```

```
        "elasticbeanstalk:List*",
        "elasticbeanstalk:RequestEnvironmentInfo",
        "elasticbeanstalk:RetrieveEnvironmentInfo",
        "elasticbeanstalk:ValidateConfigurationSettings",
        "elasticfilesystem:Describe*",
        "elasticloadbalancing:Describe*",
        "elasticmapreduce:Describe*",
        "elasticmapreduce:List*",
        "elastictranscoder:List*",
        "elastictranscoder:ReadJob",
        "elasticfilesystem:DescribeFileSystems",
        "es:Describe*",
        "es:List*",
        "es:ESHttpGet",
        "es:ESHttpHead",
        "events:DescribeRule",
        "events:List*",
        "events:TestEventPattern",
        "firehose:Describe*",
        "firehose:List*",
        "gamelift:List*",
        "gamelift:Describe*",
        "glacier:ListVaults",
        "glacier:DescribeVault",
        "glacier:DescribeJob",
        "glacier:Get*",
        "glacier:List*",
        "iam:GenerateCredentialReport",
        "iam:GenerateServiceLastAccessedDetails",
        "iam:Get*",
        "iam:List*",
        "importexport:GetStatus",
        "importexport:ListJobs",
        "inspector:Describe*",
        "inspector:List*",
        "iot:Describe*",
        "iot:Get*",
        "iot:List*",
        "kinesisanalytics:DescribeApplication",
        "kinesisanalytics:DiscoverInputSchema",
        "kinesisanalytics:GetApplicationState",
        "kinesisanalytics:ListApplications",
        "kinesis:Describe*",
        "kinesis:Get*",
```

```
        "kinesis:List*",
        "kms:Describe*",
        "kms:Get*",
        "kms:List*",
        "lambda:List*",
        "lambda:Get*",
        "logs:Describe*",
        "logs:TestMetricFilter",
        "machinelearning:Describe*",
        "machinelearning:Get*",
        "opsworks:Describe*",
        "rds:Describe*",
        "rds:ListTagsForResource",
        "redshift:Describe*",
        "rolesanywhere:GetCrl",
        "rolesanywhere:GetProfile",
        "rolesanywhere:GetSubject",
        "rolesanywhere:GetTrustAnchor",
        "rolesanywhere:ListCrls",
        "rolesanywhere:ListProfiles",
        "rolesanywhere:ListSubjects",
        "rolesanywhere:ListTagsForResource",
        "rolesanywhere:ListTrustAnchors",
        "route53:Get*",
        "route53:List*",
        "route53domains:CheckDomainAvailability",
        "route53domains:GetDomainDetail",
        "route53domains:GetOperationDetail",
        "route53domains:List*",
        "s3:List*",
        "sdb:GetAttributes",
        "sdb:List*",
        "sdb:Select*",
        "servicecatalog:SearchProducts",
        "servicecatalog:DescribeProduct",
        "servicecatalog:DescribeProductView",
        "servicecatalog:ListLaunchPaths",
        "servicecatalog:DescribeProvisioningParameters",
        "servicecatalog:ListRecordHistory",
        "servicecatalog:DescribeRecord",
        "servicecatalog:ScanProvisionedProducts",
        "ses:Get*",
        "ses:List*",
        "sns:Get*",
```

```
        "sns:List*",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ListQueues",
        "sqs:ReceiveMessage",
        "ssm:List*",
        "ssm:Describe*",
        "storagegateway:Describe*",
        "storagegateway:List*",
        "swf:Count*",
        "swf:Describe*",
        "swf:Get*",
        "swf:List*",
        "waf:Get*",
        "waf:List*",
        "workdocs:Describe*",
        "workmail:Describe*",
        "workmail:Get*",
        "workspaces:Describe*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

SystemAdministrator

説明: アプリケーションおよび開発業務向けリソースに必要なフルアクセスを付与します。

`SystemAdministrator` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに SystemAdministrator をアタッチできます。

ポリシーの詳細

- タイプ: ジョブ機能ポリシー
- 作成日時: 2016 年 11 月 10 日 17:23 UTC
- 編集日時: 2025 年 7 月 24 日 12:22 UTC
- ARN: arn:aws:iam::aws:policy/job-function/SystemAdministrator

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Statement" : [
    {
      "Action" : [
        "acm:Describe*",
        "acm:Get*",
        "acm:List*",
        "acm:Request*",
        "acm:Resend*",
        "autoscaling:*",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:ListPublicKeys",
        "cloudtrail:ListTags",
        "cloudtrail:LookupEvents",
        "cloudtrail:StartLogging",
        "cloudtrail:StopLogging",
        "cloudwatch:*",
        "codecommit:BatchGetRepositories",
```

```
        "codecommit:CreateBranch",
        "codecommit:CreateRepository",
        "codecommit:Get*",
        "codecommit:GitPull",
        "codecommit:GitPush",
        "codecommit:List*",
        "codecommit:Put*",
        "codecommit:Test*",
        "codecommit:Update*",
        "codedeploy:*",
        "codepipeline:*",
        "config:*",
        "ds:*",
        "ec2:Allocate*",
        "ec2:AssignPrivateIpAddresses*",
        "ec2:Associate*",
        "ec2:Allocate*",
        "ec2:AttachInternetGateway",
        "ec2:AttachNetworkInterface",
        "ec2:AttachVpnGateway",
        "ec2:Bundle*",
        "ec2:Cancel*",
        "ec2:Copy*",
        "ec2:CreateCustomerGateway",
        "ec2:CreateDhcpOptions",
        "ec2:CreateFlowLogs",
        "ec2:CreateImage",
        "ec2:CreateInstanceExportTask",
        "ec2:CreateInternetGateway",
        "ec2:CreateKeyPair",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion",
        "ec2:CreateNatGateway",
        "ec2:CreateNetworkInterface",
        "ec2:CreatePlacementGroup",
        "ec2:CreateReservedInstancesListing",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSnapshot",
        "ec2:CreateSpotDatafeedSubscription",
        "ec2:CreateSubnet",
        "ec2:CreateTags",
        "ec2:CreateVolume",
```

```
        "ec2:CreateVpc",
        "ec2:CreateVpcEndpoint",
        "ec2:CreateVpnConnection",
        "ec2:CreateVpnConnectionRoute",
        "ec2:CreateVpnGateway",
        "ec2:DeleteFlowLogs",
        "ec2:DeleteKeyPair",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions",
        "ec2:DeleteNatGateway",
        "ec2:DeleteNetworkInterface",
        "ec2:DeletePlacementGroup",
        "ec2:DeleteSnapshot",
        "ec2:DeleteSpotDatafeedSubscription",
        "ec2:DeleteSubnet",
        "ec2:DeleteTags",
        "ec2:DeleteVpc",
        "ec2:DeleteVpcEndpoints",
        "ec2:DeleteVpnConnection",
        "ec2:DeleteVpnConnectionRoute",
        "ec2:DeleteVpnGateway",
        "ec2:DeregisterImage",
        "ec2:Describe*",
        "ec2:DetachInternetGateway",
        "ec2:DetachNetworkInterface",
        "ec2:DetachVpnGateway",
        "ec2:DisableVgwRoutePropagation",
        "ec2:DisableVpcClassicLinkDnsSupport",
        "ec2:DisassociateAddress",
        "ec2:DisassociateRouteTable",
        "ec2:EnableVgwRoutePropagation",
        "ec2:EnableVolumeIO",
        "ec2:EnableVpcClassicLinkDnsSupport",
        "ec2:GetConsoleOutput",
        "ec2:GetHostReservationPurchasePreview",
        "ec2:GetLaunchTemplateData",
        "ec2:GetPasswordData",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:Import*",
        "ec2:Modify*",
        "ec2:MonitorInstances",
        "ec2:MoveAddressToVpc",
        "ec2:Purchase*",
        "ec2:RegisterImage",
```

```
        "ec2:Release*",
        "ec2:Replace*",
        "ec2:ReportInstanceStatus",
        "ec2:Request*",
        "ec2:Reset*",
        "ec2:RestoreAddressToClassic",
        "ec2:RunScheduledInstances",
        "ec2:UnassignPrivateIpAddresses",
        "ec2:UnmonitorInstances",
        "ec2:UpdateSecurityGroupRuleDescriptionsEgress",
        "ec2:UpdateSecurityGroupRuleDescriptionsIngress",
        "elasticloadbalancing:*",
        "events:*",
        "iam:GetAccount*",
        "iam:GetContextKeys*",
        "iam:GetCredentialReport",
        "iam:ListAccountAliases",
        "iam:ListGroups",
        "iam:ListOpenIDConnectProviders",
        "iam:ListPolicies",
        "iam:ListPoliciesGrantingServiceAccess",
        "iam:ListRoles",
        "iam:ListSAMLProviders",
        "iam:ListServerCertificates",
        "iam:Simulate*",
        "iam:UpdateServerCertificate",
        "iam:UpdateSigningCertificate",
        "kinesis:ListStreams",
        "kinesis:PutRecord",
        "kms:CreateAlias",
        "kms:CreateKey",
        "kms:DeleteAlias",
        "kms:Describe*",
        "kms:GenerateRandom",
        "kms:Get*",
        "kms:List*",
        "kms:Encrypt",
        "kms:ReEncrypt*",
        "lambda:Create*",
        "lambda:Delete*",
        "lambda:Get*",
        "lambda:InvokeFunction",
        "lambda:List*",
        "lambda:PublishVersion",
```

```
        "lambda:Update*",
        "logs:*",
        "rds:Describe*",
        "rds:ListTagsForResource",
        "rolesanywhere:GetCrl",
        "rolesanywhere:GetProfile",
        "rolesanywhere:GetSubject",
        "rolesanywhere:GetTrustAnchor",
        "rolesanywhere:ListCrls",
        "rolesanywhere:ListProfiles",
        "rolesanywhere:ListSubjects",
        "rolesanywhere:ListTagsForResource",
        "rolesanywhere:ListTrustAnchors",
        "rolesanywhere:PutNotificationSettings",
        "rolesanywhere:ResetNotificationSettings",
        "route53:*",
        "route53domains:*",
        "ses:*",
        "sns:*",
        "sqs:*",
        "trustedadvisor:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "ec2:AcceptVpcPeeringConnection",
        "ec2:AttachClassicLinkVpc",
        "ec2:AttachVolume",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateVpcPeeringConnection",
        "ec2:DeleteCustomerGateway",
        "ec2:DeleteDhcpOptions",
        "ec2:DeleteInternetGateway",
        "ec2:DeleteNetworkAcl*",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteVolume",
        "ec2:DeleteVpcPeeringConnection",
        "ec2:DetachClassicLinkVpc",
        "ec2:DetachVolume",
```

```
        "ec2:DisableVpcClassicLink",
        "ec2:EnableVpcClassicLink",
        "ec2:GetConsoleScreenshot",
        "ec2:RebootInstances",
        "ec2:RejectVpcPeeringConnection",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Action" : "s3:*",
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Action" : [
        "iam:GetAccessKeyLastUsed",
        "iam:GetGroup*",
        "iam:GetInstanceProfile",
        "iam:GetLoginProfile",
        "iam:GetOpenIDConnectProvider",
        "iam:GetPolicy*",
        "iam:GetRole*",
        "iam:GetSAMLProvider",
        "iam:GetSSHPublicKey",
        "iam:GetServerCertificate",
        "iam:GetServiceLastAccessed*",
        "iam:GetUser*",
        "iam:ListAccessKeys",
        "iam:ListAttached*",
        "iam:ListEntitiesForPolicy",
        "iam:ListGroupPolicies",
        "iam:ListGroupsForUser",
        "iam:ListInstanceProfiles*",
```

```
        "iam:ListMFADevices",
        "iam:ListPolicyVersions",
        "iam:ListRolePolicies",
        "iam:ListSSHPublicKeys",
        "iam:ListSigningCertificates",
        "iam:ListUserPolicies",
        "iam:Upload*"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Action" : [
        "iam:GetRole",
        "iam:ListRoles",
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/rds-monitoring-role",
        "arn:aws:iam::*:role/ec2-sysadmin-*",
        "arn:aws:iam::*:role/ecr-sysadmin-*",
        "arn:aws:iam::*:role/lambda-sysadmin-*"
      ]
    }
  ],
  "Version" : "2012-10-17"
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

TranslateFullAccess

説明: Amazon Translate へのフルアクセスを提供します。

TranslateFullAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに TranslateFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 11 月 27 日 23:36 UTC
- 編集日時: 2020 年 1 月 8 日 21:22 UTC
- ARN: arn:aws:iam::aws:policy/TranslateFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

TranslateReadOnly

説明: Amazon Translate への読み取り専用アクセスを提供します。

`TranslateReadOnly` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `TranslateReadOnly` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 11 月 29 日 18:22 UTC
- 編集日時: 2023 年 5 月 24 日 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/TranslateReadOnly`

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

ViewOnlyAccess

説明: このポリシーは、すべての AWS サービスのリソースと基本メタデータを表示するアクセス許可を付与します。

`ViewOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに ViewOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: ジョブ機能ポリシー
- 作成日時: 2016 年 11 月 10 日 17:20 UTC
- 編集日時: 2025 年 10 月 13 日 21:34 UTC
- ARN: arn:aws:iam::aws:policy/job-function/ViewOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v27 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GeneralViewOnlyAccessStatement",
      "Effect" : "Allow",
      "Action" : [
        "acm:ListCertificates",
        "aiops:GetInvestigation",
        "aiops:GetInvestigationGroup",
        "aiops:ListInvestigationEvents",
        "aiops:ListInvestigationGroups",
        "aiops:ListInvestigations",
        "athena:List*",
        "autoscaling:Describe*",
        "aws-marketplace:ViewSubscriptions",
        "backup:DescribeBackupJob",
        "backup:DescribeBackupVault",
        "backup:DescribeCopyJob",
```

```
        "backup:DescribeFramework",
        "backup:DescribeGlobalSettings",
        "backup:DescribeProtectedResource",
        "backup:DescribeRecoveryPoint",
        "backup:DescribeRegionSettings",
        "backup:DescribeReportJob",
        "backup:DescribeReportPlan",
        "backup:DescribeRestoreJob",
        "backup:GetSupportedResourceTypes",
        "backup:ListBackupJobs",
        "backup:ListBackupPlans",
        "backup:ListBackupPlanTemplates",
        "backup:ListBackupPlanVersions",
        "backup:ListBackupSelections",
        "backup:ListBackupVaults",
        "backup:ListCopyJobs",
        "backup:ListFrameworks",
        "backup:ListLegalHolds",
        "backup:ListProtectedResources",
        "backup:ListProtectedResourcesByBackupVault",
        "backup:ListRecoveryPointsByBackupVault",
        "backup:ListRecoveryPointsByLegalHold",
        "backup:ListRecoveryPointsByResource",
        "backup:ListReportJobs",
        "backup:ListReportPlans",
        "backup:ListRestoreJobs",
        "backup:ListTags",
        "batch:ListJobs",
        "bedrock:ListCustomModels",
        "bedrock:ListTagsForResource",
        "clouddirectory:ListAppliedSchemaArns",
        "clouddirectory:ListDevelopmentSchemaArns",
        "clouddirectory:ListDirectories",
        "clouddirectory:ListPublishedSchemaArns",
        "cloudformation:DescribeStacks",
        "cloudformation:List*",
        "cloudfront:List*",
        "cloudsearch:DescribeDomains",
        "cloudsearch:List*",
        "cloudtrail:DescribeTrails",
        "cloudtrail:ListTrails",
        "cloudtrail:LookupEvents",
        "cloudwatch:Get*",
        "cloudwatch:List*",
```

```
        "codebuild:ListBuilds*",
        "codebuild:ListProjects",
        "codecommit:List*",
        "codedeploy:BatchGetApplicationRevisions",
        "codedeploy:BatchGetApplications",
        "codedeploy:BatchGetDeploymentGroups",
        "codedeploy:BatchGetDeploymentInstances",
        "codedeploy:BatchGetDeployments",
        "codedeploy:BatchGetDeploymentTargets",
        "codedeploy:BatchGetOnPremisesInstances",
        "codedeploy:Get*",
        "codedeploy:List*",
        "codepipeline:ListPipelines",
        "codestar:List*",
        "cognito-identity:ListIdentities",
        "cognito-identity:ListIdentityPools",
        "cognito-idp:List*",
        "cognito-sync:ListDatasets",
        "comprehend:Describe*",
        "comprehend:List*",
        "config:Describe*",
        "config:List*",
        "connect:List*",
        "cost-optimization-hub:GetPreferences",
        "cost-optimization-hub:GetRecommendation",
        "cost-optimization-hub:ListEnrollmentStatuses",
        "cost-optimization-hub:ListRecommendations",
        "cost-optimization-hub:ListRecommendationSummaries",
        "databrew:ListJobs",
        "databrew:ListProjects",
        "datapipeline:DescribePipelines",
        "datapipeline:GetAccountLimits",
        "datapipeline:ListPipelines",
        "dax:DescribeClusters",
        "dax:DescribeDefaultParameters",
        "dax:DescribeEvents",
        "dax:DescribeParameterGroups",
        "dax:DescribeParameters",
        "dax:DescribeSubnetGroups",
        "dax:ListTags",
        "devicefarm:List*",
        "directconnect:Describe*",
        "discovery:List*",
        "dms:List*",
```

```
        "ds:DescribeDirectories",
        "dynamodb:DescribeBackup",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeGlobalTable",
        "dynamodb:DescribeGlobalTableSettings",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeReservedCapacity",
        "dynamodb:DescribeReservedCapacityOfferings",
        "dynamodb:DescribeStream",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:ListBackups",
        "dynamodb:ListExports",
        "dynamodb:ListGlobalTables",
        "dynamodb:ListStreams",
        "dynamodb:ListTables",
        "dynamodb:ListTagsOfResource",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeBundleTasks",
        "ec2:DescribeCarrierGateways",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeConversionTasks",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeExportTasks",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeHost*",
        "ec2:DescribeIdentityIdFormat",
        "ec2:DescribeIdFormat",
        "ec2:DescribeImage*",
        "ec2:DescribeImport*",
        "ec2:DescribeInstance*",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeLocalGateways",
        "ec2:DescribeLocalGatewayVirtualInterfaceGroups",
        "ec2:DescribeLocalGatewayVirtualInterfaces",
        "ec2:DescribeMovingAddresses",
        "ec2:DescribeNatGateways",
```

```
        "ec2:DescribeNetwork*",
        "ec2:DescribePlacementGroups",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
        "ec2:DescribeReserved*",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshot*",
        "ec2:DescribeSpot*",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVolume*",
        "ec2:DescribeVpc*",
        "ec2:DescribeVpnGateways",
        "ec2:SearchLocalGatewayRoutes",
        "ecr:DescribeRegistry",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "ecs:Describe*",
        "ecs:List*",
        "eks:ListTagsForResource",
        "elasticache:Describe*",
        "elasticbeanstalk:DescribeApplications",
        "elasticbeanstalk:DescribeApplicationVersions",
        "elasticbeanstalk:DescribeEnvironments",
        "elasticbeanstalk:ListAvailableSolutionStacks",
        "elasticfilesystem:DescribeFileSystems",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticmapreduce:List*",
        "elastictranscoder:List*",
        "emr-serverless:ListApplications",
        "es:DescribeElasticsearchDomain",
        "es:DescribeElasticsearchDomains",
        "es:ListDomainNames",
        "events:ListRuleNamesByTarget",
        "events:ListRules",
        "events:ListTargetsByRule",
        "firehose:DescribeDeliveryStream",
```

```
        "firehose:List*",
        "fsx:DescribeFileSystems",
        "gamelift:List*",
        "glacier:List*",
        "glue:GetTags",
        "greengrass:List*",
        "iam:GetAccountSummary",
        "iam:GetLoginProfile",
        "iam:List*",
        "importexport:ListJobs",
        "inspector:List*",
        "iot:List*",
        "kafka:ListClusters",
        "kendra:ListDataSources",
        "kendra:ListTagsForResource",
        "kinesis:ListStreams",
        "kinesisanalytics:ListApplications",
        "kinesisanalytics:ListTagsForResource",
        "kms:ListKeys",
        "kms:ListResourceTags",
        "lambda:List*",
        "lex:GetBotAliases",
        "lex:GetBotChannelAssociations",
        "lex:GetBots",
        "lex:GetBotVersions",
        "lex:GetIntents",
        "lex:GetIntentVersions",
        "lex:GetSlotTypes",
        "lex:GetSlotTypeVersions",
        "lex:GetUtterancesView",
        "lightsail:GetBlueprints",
        "lightsail:GetBundles",
        "lightsail:GetInstances",
        "lightsail:GetInstanceSnapshots",
        "lightsail:GetKeyPair",
        "lightsail:GetRegions",
        "lightsail:GetStaticIps",
        "lightsail:IsVpcPeered",
        "logs:Describe*",
        "logs:GetTransformer",
        "logs:ListEntitiesForLogGroup",
        "logs:ListLogGroupsForEntity",
        "logs:ListLogGroupsForQuery",
        "logs:ListTagsForResource",
```

```
        "lookoutvision:ListModelPackagingJobs",
        "lookoutvision:ListModels",
        "lookoutvision:ListProjects",
        "m2:GetApplication",
        "m2:GetEnvironment",
        "m2:ListApplications",
        "m2:ListEnvironments",
        "m2:ListTagsForResource",
        "machinelearning:Describe*",
        "mediaconnect:ListEntitlements",
        "mediaconnect:ListFlows",
        "mediaconnect:ListOfferings",
        "mediaconnect:ListReservations",
        "mobiletargeting:GetApplicationSettings",
        "mobiletargeting:GetCampaigns",
        "mobiletargeting:GetImportJobs",
        "mobiletargeting:GetSegments",
        "oam:ListAttachedLinks",
        "oam:ListLinks",
        "oam:ListSinks",
        "opsworks-cm:Describe*",
        "opsworks:Describe*",
        "organizations:List*",
        "outposts:GetOutpost",
        "outposts:GetOutpostInstanceTypes",
        "outposts:ListOutposts",
        "outposts:ListSites",
        "outposts:ListTagsForResource",
        "polly:Describe*",
        "polly:List*",
        "profile:ListDomains",
        "profile:ListIntegrations",
        "rds:Describe*",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:ListWorkgroups",
        "redshift:DescribeClusters",
        "redshift:DescribeEvents",
        "redshift:ViewQueriesInConsole",
        "resource-explorer-2:GetDefaultView",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListSupportedResourceTypes",
        "resource-explorer-2:ListTagsForResource",
        "resource-explorer-2:ListViews",
```

```
        "rolesanywhere:ListCrls",
        "rolesanywhere:ListProfiles",
        "rolesanywhere:ListSubjects",
        "rolesanywhere:ListTagsForResource",
        "rolesanywhere:ListTrustAnchors",
        "route53:Get*",
        "route53:List*",
        "route53domains:List*",
        "route53profiles:GetProfile",
        "route53profiles:GetProfileAssociation",
        "route53profiles:GetProfileResourceAssociation",
        "route53profiles:ListProfileAssociations",
        "route53profiles:ListProfileResourceAssociations",
        "route53profiles:ListProfiles",
        "route53profiles:ListTagsForResource",
        "route53resolver:Get*",
        "route53resolver:List*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListMultiRegionAccessPoints",
        "sagemaker:Describe*",
        "sagemaker:List*",
        "sdb:List*",
        "servicecatalog:List*",
        "ses:DescribeActiveReceiptRuleSet",
        "ses:List*",
        "ses:ListDedicatedIpPools",
        "shield:List*",
        "sns:List*",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ListDeadLetterSourceQueues",
        "sqs:ListMessageMoveTasks",
        "sqs:ListQueues",
        "sqs:ListQueueTags",
        "ssm:ListAssociations",
        "ssm:ListDocuments",
        "states:ListActivities",
        "states:ListExecutions",
        "states:ListMapRuns",
        "states:ListStateMachineAliases",
        "states:ListStateMachines",
        "states:ListStateMachineVersions",
        "storagegateway:ListGateways",
```

```
        "storagegateway:ListLocalDisks",
        "storagegateway:ListVolumeRecoveryPoints",
        "storagegateway:ListVolumes",
        "swf:List*",
        "trustedadvisor:Describe*",
        "waf-regional:List*",
        "waf:List*",
        "wafv2:List*",
        "workdocs:DescribeAvailableDirectories",
        "workdocs:DescribeInstances",
        "workmail:Describe*",
        "workspaces:Describe*"
      ],
      "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"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

VMImportExportRoleForAWSConnector

説明: AWS Connector を使用しているお客様向けの VM Import/Export サービスロールのデフォルトポリシー。VM Import/Export サービスは、 AWS Connector 仮想アプライアンスからの仮想マシン移行リクエストを満たすために、このポリシーを持つロールを引き受けます。(AWS コネクタは AWSConnector」管理ポリシーを使用して、お客様に代わって VM Import/Export サービスにリクエストを発行することに注意してください)。AMI および EBS スナップショットの作成、EBS スナップショットの属性の変更、EC2 オブジェクトに「Describe*」呼び出しの実行、「import-to-ec2」で始まる S3 バケットからの読み取りを行えるようにします。

VMImportExportRoleForAWSConnector は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに VMImportExportRoleForAWSConnector をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 9 月 3 日 20:48 UTC
- 編集日時: 2015 年 9 月 3 日 20:48 UTC
- ARN: arn:aws:iam::aws:policy/service-role/VMImportExportRoleForAWSConnector

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

VPCLatticeFullAccess

説明: Amazon VPC Lattice へのフルアクセス、および依存サービスへのアクセスを提供します。

`VPCLatticeFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `VPCLatticeFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 3 月 30 日 02:49 UTC
- 編集日時: 2024 年 12 月 1 日 14:21 UTC
- ARN: `arn:aws:iam::aws:policy/VPCLatticeFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:*",
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:DescribeLoadBalancers",
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams",
        "logs:DescribeLogGroups",
        "s3:ListAllMyBuckets",
        "lambda:ListAliases",
        "lambda:ListFunctions",
        "lambda:ListVersionsByFunction",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "logs:CreateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:GetLogDelivery",
        "logs:ListLogDeliveries",
        "logs:UpdateLogDelivery",
        "logs:DescribeResourcePolicies"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "vpc-lattice.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/vpc-lattice.amazonaws.com/
AWSServiceRoleForVpcLattice",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "vpc-lattice.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/delivery.logs.amazonaws.com/
AWSServiceRoleForLogDelivery",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "delivery.logs.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
```

```
      "Resource" : "arn:aws:iam::*:role/aws-service-role/vpc-lattice.amazonaws.com/
AWSServiceRoleForVpcLattice"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

VPCLatticeReadOnlyAccess

説明: 経由で Amazon VPC Lattice への読み取り専用アクセスと AWS マネジメントコンソール、依存関係サービスへの制限付きアクセスを提供します。

`VPCLatticeReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `VPCLatticeReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 3 月 30 日 02:47 UTC
- 編集日時: 2024 年 12 月 1 日 14:21 UTC
- ARN: `arn:aws:iam::aws:policy/VPCLatticeReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:Get*",
        "vpc-lattice:List*",
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "cloudwatch:GetMetricData",
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:DescribeLoadBalancers",
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams",
        "lambda:ListAliases",
        "lambda:ListFunctions",
        "lambda:ListVersionsByFunction",
        "logs:DescribeLogGroups",
        "logs:GetLogDelivery",
        "logs:ListLogDeliveries",
        "s3:ListAllMyBuckets",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

VPCLatticeServicesInvokeAccess

説明: Amazon VPC Lattice サービスを呼び出すためのアクセスを提供します。

VPCLatticeServicesInvokeAccess は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに VPCLatticeServicesInvokeAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 3 月 30 日 02:45 UTC
- 編集日時: 2023 年 3 月 30 日 02:45 UTC
- ARN: arn:aws:iam::aws:policy/VPCLatticeServicesInvokeAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice-svcs:Invoke"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

WAFLoggingServiceRolePolicy

説明: お客様のログを Firehose ストリームに書き込む SLR の作成

`WAFLoggingServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 8 月 24 日 21:05 UTC
- 編集日時: 2018 年 8 月 24 日 21:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/WAFLoggingServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : [
        "arn:aws:firehose:*:*:deliverystream/aws-waf-logs-*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

WAFRegionalLoggingServiceRolePolicy

説明: お客様のログを Firehose ストリームに書き込む SLR の作成

`WAFRegionalLoggingServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 8 月 24 日 18:40 UTC

- 編集日時: 2018 年 8 月 24 日 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/WAFRegionalLoggingServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : [
        "arn:aws:firehose:*:*:deliverystream/aws-waf-logs-*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

WAFV2LoggingServiceRolePolicy

説明: このポリシーは、 AWS WAF が Amazon Kinesis Data Firehose にログを書き込むことを許可するサービスにリンクされたロールを作成します。

WAFV2LoggingServiceRolePolicy は AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 11 月 7 日 00:40 UTC
- 編集日時: 2024 年 6 月 3 日 17:29 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/WAFV2LoggingServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

WellArchitectedConsoleFullAccess

説明: を介して AWS Well-Architected ツールへのフルアクセスを提供します AWS マネジメントコンソール

`WellArchitectedConsoleFullAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `WellArchitectedConsoleFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 11 月 29 日 18:19 UTC
- 編集日時: 2018 年 11 月 29 日 18:19 UTC
- ARN: `arn:aws:iam::aws:policy/WellArchitectedConsoleFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "wellarchitected:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

WellArchitectedConsoleReadOnlyAccess

説明: を介して AWS Well-Architected ツールへの読み取り専用アクセスを提供します AWS マネジメントコンソール

`WellArchitectedConsoleReadOnlyAccess` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `WellArchitectedConsoleReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 11 月 29 日 18:21 UTC
- 編集日時: 2023 年 6 月 29 日 17:16 UTC
- ARN: `arn:aws:iam::aws:policy/WellArchitectedConsoleReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "wellarchitected:Get*",
        "wellarchitected:List*",
        "wellarchitected:ExportLens"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

WorkLinkServiceRolePolicy

説明: Amazon WorkLink が使用または管理する AWS のサービス および リソースへのアクセスを有効にします

`WorkLinkServiceRolePolicy` は AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `WorkLinkServiceRolePolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 1 月 23 日 19:03 UTC
- 編集日時: 2019 年 1 月 23 日 19:03 UTC
- ARN: `arn:aws:iam::aws:policy/WorkLinkServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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-*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。