Panduan Referensi

AWS Kebijakan Terkelola

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

AWS Kebijakan Terkelola: Panduan Referensi

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

Merek dagang dan tampilan dagang Amazon tidak boleh digunakan sehubungan dengan produk atau layanan apa pun yang bukan milik Amazon, dengan cara apa pun yang dapat menyebabkan kebingungan di antara pelanggan, atau dengan cara apa pun yang merendahkan atau mendiskreditkan Amazon. Semua merek dagang lain yang tidak dimiliki oleh Amazon merupakan hak milik masing-masing pemiliknya, yang mungkin atau tidak terafiliasi, terkait dengan, atau disponsori oleh Amazon.

Table of Contents

Apa itu kebijakan yang AWS dikelola? 1
Memahami halaman referensi kebijakan 1
Kebijakan terkelola yang tidak digunakan lagi AWS 2
AWS kebijakan terkelola 3
AccessAnalyzerServiceRolePolicy 49
Menggunakan kebijakan ini 49
Rincian kebijakan 49
Versi kebijakan 49
Dokumen kebijakan JSON 50
Pelajari selengkapnya 52
AdministratorAccess 52
Menggunakan kebijakan ini 52
Rincian kebijakan 53
Versi kebijakan 53
Dokumen kebijakan JSON 53
Pelajari selengkapnya 53
AdministratorAccess-Amplify 54
Menggunakan kebijakan ini 54
Rincian kebijakan 54
Versi kebijakan 54
Dokumen kebijakan JSON 54
Pelajari selengkapnya 65
AdministratorAccess-AWSElasticBeanstalk 65
Menggunakan kebijakan ini 65
Rincian kebijakan 65
Versi kebijakan 65
Dokumen kebijakan JSON 66
Pelajari selengkapnya 74
AIOpsAssistantPolicy 74
Menggunakan kebijakan ini 74
Rincian kebijakan 74
Versi kebijakan 74
Dokumen kebijakan JSON 75
Pelajari selengkapnya 95

AIOpsConsoleAdminPolicy 95
Menggunakan kebijakan ini 95
Rincian kebijakan 95
Versi kebijakan 96
Dokumen kebijakan JSON 96
Pelajari selengkapnya 101
AIOpsOperatorAccess 102
Menggunakan kebijakan ini 102
Rincian kebijakan 102
Versi kebijakan 102
Dokumen kebijakan JSON 102
Pelajari selengkapnya 105
AIOpsReadOnlyAccess 105
Menggunakan kebijakan ini 105
Rincian kebijakan 105
Versi kebijakan 106
Dokumen kebijakan JSON 106
Pelajari selengkapnya 106
AlexaForBusinessDeviceSetup 107
Menggunakan kebijakan ini 107
Rincian kebijakan 107
Versi kebijakan 107
Dokumen kebijakan JSON 107
Pelajari selengkapnya 108
AlexaForBusinessFullAccess 108
Menggunakan kebijakan ini 108
Rincian kebijakan 108
Versi kebijakan 109
Dokumen kebijakan JSON 109
Pelajari selengkapnya 110
AlexaForBusinessGatewayExecution 110
Menggunakan kebijakan ini 111
Rincian kebijakan 111
Versi kebijakan 111
Dokumen kebijakan JSON 111
Pelajari selengkapnya 112

AlexaForBusinessLifesizeDelegatedAccessPolicy 112
Menggunakan kebijakan ini 112
Rincian kebijakan 112
Versi kebijakan 113
Dokumen kebijakan JSON 113
Pelajari selengkapnya 115
AlexaForBusinessNetworkProfileServicePolicy 115
Menggunakan kebijakan ini 116
Rincian kebijakan 116
Versi kebijakan 116
Dokumen kebijakan JSON 116
Pelajari selengkapnya 117
AlexaForBusinessPolyDelegatedAccessPolicy 117
Menggunakan kebijakan ini 117
Rincian kebijakan 117
Versi kebijakan 117
Dokumen kebijakan JSON 118
Pelajari selengkapnya 119
AlexaForBusinessReadOnlyAccess 120
Menggunakan kebijakan ini 120
Rincian kebijakan 120
Versi kebijakan 120
Dokumen kebijakan JSON 120
Pelajari selengkapnya 121
AmazonAPIGatewayAdministrator 121
Menggunakan kebijakan ini 121
Rincian kebijakan 121
Versi kebijakan 121
Dokumen kebijakan JSON 122
Pelajari selengkapnya 122
AmazonAPIGatewayInvokeFullAccess 122
Menggunakan kebijakan ini 122
Rincian kebijakan 122
Versi kebijakan 123
Dokumen kebijakan JSON 123
Pelajari selengkapnya 123

AmazonAPIGatewayPushToCloudWatchLogs 123
Menggunakan kebijakan ini 124
Rincian kebijakan 124
Versi kebijakan 124
Dokumen kebijakan JSON 124
Pelajari selengkapnya 125
AmazonAppFlowFullAccess 125
Menggunakan kebijakan ini 125
Rincian kebijakan 125
Versi kebijakan 125
Dokumen kebijakan JSON 126
Pelajari selengkapnya 128
AmazonAppFlowReadOnlyAccess 129
Menggunakan kebijakan ini 129
Rincian kebijakan 129
Versi kebijakan 129
Dokumen kebijakan JSON 129
Pelajari selengkapnya 130
AmazonAppStreamFullAccess 130
Menggunakan kebijakan ini 130
Rincian kebijakan 130
Versi kebijakan 130
Dokumen kebijakan JSON 131
Pelajari selengkapnya 132
AmazonAppStreamPCAAccess 133
Menggunakan kebijakan ini 133
Rincian kebijakan 133
Versi kebijakan 133
Dokumen kebijakan JSON 133
Pelajari selengkapnya 134
AmazonAppStreamReadOnlyAccess 134
Menggunakan kebijakan ini 134
Rincian kebijakan 134
Versi kebijakan 135
Dokumen kebijakan JSON 135
Pelajari selengkapnya 135

AmazonAppStreamServiceAccess 135
Menggunakan kebijakan ini 136
Rincian kebijakan 136
Versi kebijakan 136
Dokumen kebijakan JSON 136
Pelajari selengkapnya 137
AmazonAthenaFullAccess 137
Menggunakan kebijakan ini 138
Rincian kebijakan 138
Versi kebijakan 138
Dokumen kebijakan JSON 138
Pelajari selengkapnya 141
AmazonAugmentedAIFullAccess 142
Menggunakan kebijakan ini 142
Rincian kebijakan 142
Versi kebijakan 142
Dokumen kebijakan JSON 142
Pelajari selengkapnya 143
AmazonAugmentedAIHumanLoopFullAccess 144
Menggunakan kebijakan ini 144
Rincian kebijakan 144
Versi kebijakan 144
Dokumen kebijakan JSON 144
Pelajari selengkapnya 145
AmazonAugmentedAIIntegratedAPIAccess 145
Menggunakan kebijakan ini 145
Rincian kebijakan 145
Versi kebijakan 145
Dokumen kebijakan JSON 146
Pelajari selengkapnya 147
AmazonAuroraDSQLConsoleFullAccess 147
Menggunakan kebijakan ini 147
Rincian kebijakan 147
Versi kebijakan 148
Dokumen kebijakan JSON 148
Pelajari selengkapnya 150

AmazonAuroraDSQLFullAccess 150
Menggunakan kebijakan ini 150
Rincian kebijakan 150
Versi kebijakan 150
Dokumen kebijakan JSON 151
Pelajari selengkapnya 153
AmazonAuroraDSQLReadOnlyAccess 153
Menggunakan kebijakan ini 153
Rincian kebijakan 153
Versi kebijakan 153
Dokumen kebijakan JSON 154
Pelajari selengkapnya 154
AmazonBedrockFullAccess 154
Menggunakan kebijakan ini 155
Rincian kebijakan 155
Versi kebijakan 155
Dokumen kebijakan JSON 155
Pelajari selengkapnya 160
AmazonBedrockLimitedAccess 160
Menggunakan kebijakan ini 160
Rincian kebijakan 161
Versi kebijakan 161
Dokumen kebijakan JSON 161
Pelajari selengkapnya 163
AmazonBedrockMarketplaceAccess 163
Menggunakan kebijakan ini 163
Rincian kebijakan 163
Versi kebijakan 164
Dokumen kebijakan JSON 164
Pelajari selengkapnya 168
AmazonBedrockReadOnly 168
Menggunakan kebijakan ini 168
Rincian kebijakan 168
Versi kebijakan 169
Dokumen kebijakan JSON 169
Pelajari selengkapnya 170

AmazonBedrockStudioPermissionsBoundary 170
Menggunakan kebijakan ini 171
Rincian kebijakan 171
Versi kebijakan 171
Dokumen kebijakan JSON 171
Pelajari selengkapnya 175
AmazonBraketFullAccess 175
Menggunakan kebijakan ini 176
Rincian kebijakan 176
Versi kebijakan 176
Dokumen kebijakan JSON 176
Pelajari selengkapnya 180
AmazonBraketJobsExecutionPolicy 181
Menggunakan kebijakan ini 181
Rincian kebijakan 181
Versi kebijakan 181
Dokumen kebijakan JSON 181
Pelajari selengkapnya 184
AmazonBraketServiceRolePolicy 184
Menggunakan kebijakan ini 184
Rincian kebijakan 184
Versi kebijakan 185
Dokumen kebijakan JSON 185
Pelajari selengkapnya 185
AmazonChimeFullAccess 186
Menggunakan kebijakan ini 186
Rincian kebijakan 186
Versi kebijakan 186
Dokumen kebijakan JSON 186
Pelajari selengkapnya 188
AmazonChimeReadOnly 189
Menggunakan kebijakan ini 189
Rincian kebijakan 189
Versi kebijakan 189
Dokumen kebijakan JSON 189
Pelajari selengkapnya 190

AmazonChimeSDK 190
Menggunakan kebijakan ini 190
Rincian kebijakan 190
Versi kebijakan 190
Dokumen kebijakan JSON 191
Pelajari selengkapnya 192
AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy 192
Menggunakan kebijakan ini 192
Rincian kebijakan 192
Versi kebijakan 192
Dokumen kebijakan JSON 193
Pelajari selengkapnya 194
AmazonChimeSDKMessagingServiceRolePolicy 194
Menggunakan kebijakan ini 194
Rincian kebijakan 194
Versi kebijakan 195
Dokumen kebijakan JSON 195
Pelajari selengkapnya 196
AmazonChimeServiceRolePolicy 196
Menggunakan kebijakan ini 196
Rincian kebijakan 196
Versi kebijakan 196
Dokumen kebijakan JSON 196
Pelajari selengkapnya 197
AmazonChimeTranscriptionServiceLinkedRolePolicy 197
Menggunakan kebijakan ini 197
Rincian kebijakan 197
Versi kebijakan 198
Dokumen kebijakan JSON 198
Pelajari selengkapnya 198
AmazonChimeUserManagement 198
Menggunakan kebijakan ini 199
Rincian kebijakan 199
Versi kebijakan 199
Dokumen kebijakan JSON 199
Pelajari selengkapnya 200

AmazonChimeVoiceConnectorServiceLinkedRolePolicy 201
Menggunakan kebijakan ini 201
Rincian kebijakan 201
Versi kebijakan 201
Dokumen kebijakan JSON 201
Pelajari selengkapnya 203
AmazonCloudDirectoryFullAccess 203
Menggunakan kebijakan ini 203
Rincian kebijakan 203
Versi kebijakan 204
Dokumen kebijakan JSON 204
Pelajari selengkapnya 204
AmazonCloudDirectoryReadOnlyAccess 205
Menggunakan kebijakan ini 205
Rincian kebijakan 205
Versi kebijakan 205
Dokumen kebijakan JSON 205
Pelajari selengkapnya 206
AmazonCloudWatchEvidentlyFullAccess 206
Menggunakan kebijakan ini 206
Rincian kebijakan 206
Versi kebijakan 206
Dokumen kebijakan JSON 207
Pelajari selengkapnya 209
AmazonCloudWatchEvidentlyReadOnlyAccess 209
Menggunakan kebijakan ini 209
Rincian kebijakan 210
Versi kebijakan 210
Dokumen kebijakan JSON 210
Pelajari selengkapnya 210
AmazonCloudWatchEvidentlyServiceRolePolicy 211
Menggunakan kebijakan ini 211
Rincian kebijakan 211
Versi kebijakan 211
Dokumen kebijakan JSON 211
Pelajari selengkapnya 213

AmazonCloudWatchRUMFullAccess 213
Menggunakan kebijakan ini 213
Rincian kebijakan 213
Versi kebijakan 213
Dokumen kebijakan JSON 214
Pelajari selengkapnya 216
AmazonCloudWatchRUMReadOnlyAccess 216
Menggunakan kebijakan ini 216
Rincian kebijakan 217
Versi kebijakan 217
Dokumen kebijakan JSON 217
Pelajari selengkapnya 218
AmazonCloudWatchRUMServiceRolePolicy 219
Menggunakan kebijakan ini 219
Rincian kebijakan 219
Versi kebijakan 219
Dokumen kebijakan JSON 219
Pelajari selengkapnya 220
AmazonCodeCatalystFullAccess 220
Menggunakan kebijakan ini 220
Rincian kebijakan 220
Versi kebijakan 221
Dokumen kebijakan JSON 221
Pelajari selengkapnya 222
AmazonCodeCatalystReadOnlyAccess 222
Menggunakan kebijakan ini 222
Rincian kebijakan 222
Versi kebijakan 222
Dokumen kebijakan JSON 223
Pelajari selengkapnya 223
AmazonCodeCatalystSupportAccess 223
Menggunakan kebijakan ini 223
Rincian kebijakan 223
Versi kebijakan 224
Dokumen kebijakan JSON 224
Pelajari selengkapnya 225

AmazonCodeGuruProfilerAgentAccess 225
Menggunakan kebijakan ini 225
Rincian kebijakan 225
Versi kebijakan 225
Dokumen kebijakan JSON 225
Pelajari selengkapnya 226
AmazonCodeGuruProfilerFullAccess 226
Menggunakan kebijakan ini 226
Rincian kebijakan 226
Versi kebijakan 227
Dokumen kebijakan JSON 227
Pelajari selengkapnya 227
AmazonCodeGuruProfilerReadOnlyAccess 228
Menggunakan kebijakan ini 228
Rincian kebijakan 228
Versi kebijakan 228
Dokumen kebijakan JSON 228
Pelajari selengkapnya 229
AmazonCodeGuruReviewerFullAccess 229
Menggunakan kebijakan ini 229
Rincian kebijakan 229
Versi kebijakan 230
Dokumen kebijakan JSON 230
Pelajari selengkapnya 232
AmazonCodeGuruReviewerReadOnlyAccess 232
Menggunakan kebijakan ini 233
Rincian kebijakan 233
Versi kebijakan 233
Dokumen kebijakan JSON 233
Pelajari selengkapnya 234
AmazonCodeGuruReviewerServiceRolePolicy 234
Menggunakan kebijakan ini 234
Rincian kebijakan 234
Versi kebijakan 234
Dokumen kebijakan JSON 235
Pelajari selengkapnya 237

AmazonCodeGuruSecurityFullAccess 237
Menggunakan kebijakan ini 237
Rincian kebijakan 237
Versi kebijakan 237
Dokumen kebijakan JSON 237
Pelajari selengkapnya 238
AmazonCodeGuruSecurityScanAccess 238
Menggunakan kebijakan ini 238
Rincian kebijakan 238
Versi kebijakan 238
Dokumen kebijakan JSON 239
Pelajari selengkapnya 239
AmazonCognitoDeveloperAuthenticatedIdentities 239
Menggunakan kebijakan ini 240
Rincian kebijakan 240
Versi kebijakan 240
Dokumen kebijakan JSON 240
Pelajari selengkapnya 241
AmazonCognitoIdpEmailServiceRolePolicy 241
Menggunakan kebijakan ini 241
Rincian kebijakan 241
Versi kebijakan 241
Dokumen kebijakan JSON 242
Pelajari selengkapnya 242
AmazonCognitoIdpServiceRolePolicy 242
Menggunakan kebijakan ini 242
Rincian kebijakan 243
Versi kebijakan 243
Dokumen kebijakan JSON 243
Pelajari selengkapnya 243
AmazonCognitoPowerUser 244
Menggunakan kebijakan ini 244
Rincian kebijakan 244
Versi kebijakan 244
Dokumen kebijakan JSON 244
Pelajari selengkapnya 246

AmazonCognitoReadOnly 246
Menggunakan kebijakan ini 246
Rincian kebijakan 246
Versi kebijakan 246
Dokumen kebijakan JSON 246
Pelajari selengkapnya 247
AmazonCognitoUnAuthedIdentitiesSessionPolicy 247
Menggunakan kebijakan ini 248
Rincian kebijakan 248
Versi kebijakan 248
Dokumen kebijakan JSON 248
Pelajari selengkapnya 249
AmazonCognitoUnauthenticatedIdentities 249
Menggunakan kebijakan ini 250
Rincian kebijakan 250
Versi kebijakan 250
Dokumen kebijakan JSON 250
Pelajari selengkapnya 251
AmazonConnect_FullAccess 251
Menggunakan kebijakan ini 251
Rincian kebijakan 251
Versi kebijakan 251
Dokumen kebijakan JSON 252
Pelajari selengkapnya 254
AmazonConnectCampaignsServiceLinkedRolePolicy 254
Menggunakan kebijakan ini 255
Rincian kebijakan 255
Versi kebijakan 255
Dokumen kebijakan JSON 255
Pelajari selengkapnya 257
AmazonConnectReadOnlyAccess 257
Menggunakan kebijakan ini 257
Rincian kebijakan 257
Versi kebijakan 258
Dokumen kebijakan JSON 258
Pelajari selengkapnya 258

AmazonConnectServiceLinkedRolePolicy 259
Menggunakan kebijakan ini 259
Rincian kebijakan 259
Versi kebijakan 259
Dokumen kebijakan JSON 259
Pelajari selengkapnya 270
AmazonConnectSynchronizationServiceRolePolicy 270
Menggunakan kebijakan ini 270
Rincian kebijakan 270
Versi kebijakan 270
Dokumen kebijakan JSON 271
Pelajari selengkapnya 272
AmazonConnectVoiceIDFullAccess 273
Menggunakan kebijakan ini 273
Rincian kebijakan 273
Versi kebijakan 273
Dokumen kebijakan JSON 273
Pelajari selengkapnya 274
AmazonDataZoneBedrockModelConsumptionPolicy 274
Menggunakan kebijakan ini 274
Rincian kebijakan 274
Versi kebijakan 274
Dokumen kebijakan JSON 275
Pelajari selengkapnya 277
AmazonDataZoneBedrockModelManagementPolicy 277
Menggunakan kebijakan ini 277
Rincian kebijakan 277
Versi kebijakan 278
Dokumen kebijakan JSON 278
Pelajari selengkapnya 280
AmazonDataZoneDomainExecutionRolePolicy 280
Menggunakan kebijakan ini 280
Rincian kebijakan 280
Versi kebijakan 280
Dokumen kebijakan JSON 281
Pelajari selengkapnya 284

AmazonDataZoneEnvironmentRolePermissionsBoundary 284
Menggunakan kebijakan ini 285
Rincian kebijakan 285
Versi kebijakan 285
Dokumen kebijakan JSON 285
Pelajari selengkapnya 298
AmazonDataZoneFullAccess 298
Menggunakan kebijakan ini 298
Rincian kebijakan 298
Versi kebijakan 299
Dokumen kebijakan JSON 299
Pelajari selengkapnya 308
AmazonDataZoneFullUserAccess 308
Menggunakan kebijakan ini 308
Rincian kebijakan 308
Versi kebijakan 308
Dokumen kebijakan JSON 309
Pelajari selengkapnya 312
AmazonDataZoneGlueManageAccessRolePolicy 312
Menggunakan kebijakan ini 312
Rincian kebijakan 313
Versi kebijakan 313
Dokumen kebijakan JSON 313
Pelajari selengkapnya 321
AmazonDataZonePortalFullAccessPolicy 321
Menggunakan kebijakan ini 321
Rincian kebijakan 321
Versi kebijakan 321
Dokumen kebijakan JSON 322
Pelajari selengkapnya 322
AmazonDataZonePreviewConsoleFullAccess 322
Menggunakan kebijakan ini 322
Rincian kebijakan 322
Versi kebijakan 323
Dokumen kebijakan JSON 323
Pelajari selengkapnya 325

AmazonDataZoneProjectDeploymentPermissionsBoundary 325
Menggunakan kebijakan ini 325
Rincian kebijakan 325
Versi kebijakan 325
Dokumen kebijakan JSON 326
Pelajari selengkapnya 334
AmazonDataZoneProjectRolePermissionsBoundary 334
Menggunakan kebijakan ini 334
Rincian kebijakan 334
Versi kebijakan 334
Dokumen kebijakan JSON 334
Pelajari selengkapnya 342
AmazonDataZoneRedshiftGlueProvisioningPolicy 342
Menggunakan kebijakan ini 342
Rincian kebijakan 342
Versi kebijakan 342
Dokumen kebijakan JSON 343
Pelajari selengkapnya 350
AmazonDataZoneRedshiftManageAccessRolePolicy 351
Menggunakan kebijakan ini 351
Rincian kebijakan 351
Versi kebijakan 351
Dokumen kebijakan JSON 351
Pelajari selengkapnya 354
AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary 355
Menggunakan kebijakan ini 355
Rincian kebijakan 355
Versi kebijakan 355
Dokumen kebijakan JSON 356
Pelajari selengkapnya 383
AmazonDataZoneSageMakerManageAccessRolePolicy 383
Menggunakan kebijakan ini 383
Rincian kebijakan 383
Versi kebijakan 384
Dokumen kebijakan JSON 384
Pelajari selengkapnya 388

AmazonDataZoneSageMakerProvisioningRolePolicy 389
Menggunakan kebijakan ini 389
Rincian kebijakan 389
Versi kebijakan 389
Dokumen kebijakan JSON 389
Pelajari selengkapnya 394
AmazonDetectiveFullAccess 394
Menggunakan kebijakan ini 394
Rincian kebijakan 394
Versi kebijakan 395
Dokumen kebijakan JSON 395
Pelajari selengkapnya 396
AmazonDetectiveInvestigatorAccess 396
Menggunakan kebijakan ini 396
Rincian kebijakan 396
Versi kebijakan 396
Dokumen kebijakan JSON 397
Pelajari selengkapnya 398
AmazonDetectiveMemberAccess 398
Menggunakan kebijakan ini 399
Rincian kebijakan 399
Versi kebijakan 399
Dokumen kebijakan JSON 399
Pelajari selengkapnya 400
AmazonDetectiveOrganizationsAccess 400
Menggunakan kebijakan ini 400
Rincian kebijakan 400
Versi kebijakan 400
Dokumen kebijakan JSON 401
Pelajari selengkapnya 402
AmazonDetectiveServiceLinkedRolePolicy 402
Menggunakan kebijakan ini 403
Rincian kebijakan 403
Versi kebijakan 403
Dokumen kebijakan JSON 403
Pelajari selengkapnya 404

AmazonDevOpsGuruConsoleFullAccess 404
Menggunakan kebijakan ini 404
Rincian kebijakan 404
Versi kebijakan 404
Dokumen kebijakan JSON 404
Pelajari selengkapnya 407
AmazonDevOpsGuruFullAccess 407
Menggunakan kebijakan ini 407
Rincian kebijakan 407
Versi kebijakan 407
Dokumen kebijakan JSON 408
Pelajari selengkapnya 410
AmazonDevOpsGuruOrganizationsAccess 410
Menggunakan kebijakan ini 410
Rincian kebijakan 410
Versi kebijakan 411
Dokumen kebijakan JSON 411
Pelajari selengkapnya 412
AmazonDevOpsGuruReadOnlyAccess 412
Menggunakan kebijakan ini 412
Rincian kebijakan 412
Versi kebijakan 413
Dokumen kebijakan JSON 413
Pelajari selengkapnya 415
AmazonDevOpsGuruServiceRolePolicy 415
Menggunakan kebijakan ini 415
Rincian kebijakan 415
Versi kebijakan 415
Dokumen kebijakan JSON 416
Pelajari selengkapnya 420
AmazonDMSCloudWatchLogsRole 420
Menggunakan kebijakan ini 420
Rincian kebijakan 420
Versi kebijakan 420
Dokumen kebijakan JSON 420
Pelajari selengkapnya 422

AmazonDMSRedshiftS3Role 422
Menggunakan kebijakan ini 422
Rincian kebijakan 422
Versi kebijakan 423
Dokumen kebijakan JSON 423
Pelajari selengkapnya 423
AmazonDMSVPCManagementRole 424
Menggunakan kebijakan ini 424
Rincian kebijakan 424
Versi kebijakan 424
Dokumen kebijakan JSON 424
Pelajari selengkapnya 425
AmazonDocDB-ElasticServiceRolePolicy 425
Menggunakan kebijakan ini 425
Rincian kebijakan 425
Versi kebijakan 426
Dokumen kebijakan JSON 426
Pelajari selengkapnya 426
AmazonDocDBConsoleFullAccess 427
Menggunakan kebijakan ini 427
Rincian kebijakan 427
Versi kebijakan 427
Dokumen kebijakan JSON 427
Pelajari selengkapnya 432
AmazonDocDBElasticFullAccess 432
Menggunakan kebijakan ini 432
Rincian kebijakan 432
Versi kebijakan 432
Dokumen kebijakan JSON 433
Pelajari selengkapnya 436
AmazonDocDBElasticReadOnlyAccess 436
Menggunakan kebijakan ini 436
Rincian kebijakan 436
Versi kebijakan 436
Dokumen kebijakan JSON 437
Pelajari selengkapnya 437

AmazonDocDBFullAccess 438
Menggunakan kebijakan ini 438
Rincian kebijakan 438
Versi kebijakan 438
Dokumen kebijakan JSON 438
Pelajari selengkapnya 441
AmazonDocDBReadOnlyAccess 441
Menggunakan kebijakan ini 441
Rincian kebijakan 441
Versi kebijakan 442
Dokumen kebijakan JSON 442
Pelajari selengkapnya 444
AmazonDRSVPCManagement 444
Menggunakan kebijakan ini 444
Rincian kebijakan 444
Versi kebijakan 444
Dokumen kebijakan JSON 444
Pelajari selengkapnya 445
AmazonDynamoDBFullAccess 445
Menggunakan kebijakan ini 445
Rincian kebijakan 446
Versi kebijakan 446
Dokumen kebijakan JSON 446
Pelajari selengkapnya 449
AmazonDynamoDBFullAccess_v2 449
Menggunakan kebijakan ini 449
Rincian kebijakan 449
Versi kebijakan 449
Dokumen kebijakan JSON 449
Pelajari selengkapnya 453
AmazonDynamoDBFullAccesswithDataPipeline 453
Menggunakan kebijakan ini 453
Rincian kebijakan 453
Versi kebijakan 453
Dokumen kebijakan JSON 454
Pelajari selengkapnya 456

AmazonDynamoDBReadOnlyAccess 456
Menggunakan kebijakan ini 456
Rincian kebijakan 456
Versi kebijakan 456
Dokumen kebijakan JSON 457
Pelajari selengkapnya 458
AmazonEBSCSIDriverPolicy 458
Menggunakan kebijakan ini 459
Rincian kebijakan 459
Versi kebijakan 459
Dokumen kebijakan JSON 459
Pelajari selengkapnya 463
AmazonEC2ContainerRegistryFullAccess 463
Menggunakan kebijakan ini 464
Rincian kebijakan 464
Versi kebijakan 464
Dokumen kebijakan JSON 464
Pelajari selengkapnya 465
AmazonEC2ContainerRegistryPowerUser 465
Menggunakan kebijakan ini 465
Rincian kebijakan 465
Versi kebijakan 466
Dokumen kebijakan JSON 466
Pelajari selengkapnya 466
AmazonEC2ContainerRegistryPullOnly 467
Menggunakan kebijakan ini 467
Rincian kebijakan 467
Versi kebijakan 467
Dokumen kebijakan JSON 467
Pelajari selengkapnya 468
AmazonEC2ContainerRegistryReadOnly 468
Menggunakan kebijakan ini 468
Rincian kebijakan 468
Versi kebijakan 468
Dokumen kebijakan JSON 469
Pelajari selengkapnya 469

AmazonEC2ContainerServiceAutoscaleRole 470
Menggunakan kebijakan ini 470
Rincian kebijakan 470
Versi kebijakan 470
Dokumen kebijakan JSON 470
Pelajari selengkapnya 471
AmazonEC2ContainerServiceEventsRole 471
Menggunakan kebijakan ini 471
Rincian kebijakan 471
Versi kebijakan 472
Dokumen kebijakan JSON 472
Pelajari selengkapnya 473
AmazonEC2ContainerServiceforEC2Role 473
Menggunakan kebijakan ini 473
Rincian kebijakan 473
Versi kebijakan 474
Dokumen kebijakan JSON 474
Pelajari selengkapnya 475
AmazonEC2ContainerServiceRole 475
Menggunakan kebijakan ini 475
Rincian kebijakan 475
Versi kebijakan 475
Dokumen kebijakan JSON 476
Pelajari selengkapnya 476
AmazonEC2FullAccess 476
Menggunakan kebijakan ini 477
Rincian kebijakan 477
Versi kebijakan 477
Dokumen kebijakan JSON 477
Pelajari selengkapnya 478
AmazonEC2ReadOnlyAccess 478
Menggunakan kebijakan ini 478
Rincian kebijakan 479
Versi kebijakan 479
Dokumen kebijakan JSON 479
Pelajari selengkapnya 480

AmazonEC2RoleforAWSCodeDeploy 480
Menggunakan kebijakan ini 480
Rincian kebijakan 480
Versi kebijakan 481
Dokumen kebijakan JSON 481
Pelajari selengkapnya 481
AmazonEC2RoleforAWSCodeDeployLimited 481
Menggunakan kebijakan ini 482
Rincian kebijakan 482
Versi kebijakan 482
Dokumen kebijakan JSON 482
Pelajari selengkapnya 483
AmazonEC2RoleforDataPipelineRole 483
Menggunakan kebijakan ini 483
Rincian kebijakan 483
Versi kebijakan 484
Dokumen kebijakan JSON 484
Pelajari selengkapnya 484
AmazonEC2RoleforSSM 485
Menggunakan kebijakan ini 485
Rincian kebijakan 485
Versi kebijakan 485
Dokumen kebijakan JSON 485
Pelajari selengkapnya 488
AmazonEC2RolePolicyForLaunchWizard 488
Menggunakan kebijakan ini 488
Rincian kebijakan 488
Versi kebijakan 488
Dokumen kebijakan JSON 489
Pelajari selengkapnya 492
AmazonEC2SpotFleetAutoscaleRole 493
Menggunakan kebijakan ini 493
Rincian kebijakan 493
Versi kebijakan 493
Dokumen kebijakan JSON 493
Pelajari selengkapnya 494

AmazonEC2SpotFleetTaggingRole 495
Menggunakan kebijakan ini 495
Rincian kebijakan 495
Versi kebijakan 495
Dokumen kebijakan JSON 495
Pelajari selengkapnya 497
AmazonECS_FullAccess 497
Menggunakan kebijakan ini 497
Rincian kebijakan 497
Versi kebijakan 497
Dokumen kebijakan JSON 497
Pelajari selengkapnya 503
AmazonECSComputeServiceRolePolicy 503
Menggunakan kebijakan ini 504
Rincian kebijakan 504
Versi kebijakan 504
Dokumen kebijakan JSON 504
Pelajari selengkapnya 506
AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity 506
Menggunakan kebijakan ini 506
Rincian kebijakan 506
Versi kebijakan 506
Dokumen kebijakan JSON 507
Pelajari selengkapnya 509
AmazonECSInfrastructureRolePolicyForVolumes 509
Menggunakan kebijakan ini 509
Rincian kebijakan 509
Versi kebijakan 510
Dokumen kebijakan JSON 510
Pelajari selengkapnya 512
AmazonECSInfrastructureRolePolicyForVpcLattice 512
Menggunakan kebijakan ini 512
Rincian kebijakan 512
Versi kebijakan 513
Dokumen kebijakan JSON 513
Pelajari selengkapnya 514

AmazonECSServiceRolePolicy 514
Menggunakan kebijakan ini 514
Rincian kebijakan 515
Versi kebijakan 515
Dokumen kebijakan JSON 515
Pelajari selengkapnya 520
AmazonECSTaskExecutionRolePolicy 520
Menggunakan kebijakan ini 520
Rincian kebijakan 520
Versi kebijakan 521
Dokumen kebijakan JSON 521
Pelajari selengkapnya 521
AmazonEFSCSIDriverPolicy 522
Menggunakan kebijakan ini 522
Rincian kebijakan 522
Versi kebijakan 522
Dokumen kebijakan JSON 522
Pelajari selengkapnya 524
AmazonEKS_CNI_Policy 524
Menggunakan kebijakan ini 524
Rincian kebijakan 524
Versi kebijakan 524
Dokumen kebijakan JSON 525
Pelajari selengkapnya 526
AmazonEKSBlockStoragePolicy 526
Menggunakan kebijakan ini 526
Rincian kebijakan 526
Versi kebijakan 526
Dokumen kebijakan JSON 526
Pelajari selengkapnya 529
AmazonEKSClusterPolicy 529
Menggunakan kebijakan ini 529
Rincian kebijakan 529
Versi kebijakan 529
Dokumen kebijakan JSON 530
Pelajari selengkapnya 532

AmazonEKSComputePolicy 532
Menggunakan kebijakan ini 532
Rincian kebijakan 532
Versi kebijakan 533
Dokumen kebijakan JSON 533
Pelajari selengkapnya 535
AmazonEKSConnectorServiceRolePolicy 536
Menggunakan kebijakan ini 536
Rincian kebijakan 536
Versi kebijakan 536
Dokumen kebijakan JSON 536
Pelajari selengkapnya 538
AmazonEKSDashboardConsoleReadOnly 538
Menggunakan kebijakan ini 538
Rincian kebijakan 539
Versi kebijakan 539
Dokumen kebijakan JSON 539
Pelajari selengkapnya 540
AmazonEKSDashboardServiceRolePolicy 540
Menggunakan kebijakan ini 540
Rincian kebijakan 541
Versi kebijakan 541
Dokumen kebijakan JSON 541
Pelajari selengkapnya 542
AmazonEKSFargatePodExecutionRolePolicy 542
Menggunakan kebijakan ini 542
Rincian kebijakan 542
Versi kebijakan 542
Dokumen kebijakan JSON 542
Pelajari selengkapnya 543
AmazonEKSForFargateServiceRolePolicy 543
Menggunakan kebijakan ini 543
Rincian kebijakan 543
Versi kebijakan 544
Dokumen kebijakan JSON 544
Pelajari selengkapnya 544

AmazonEKSLoadBalancingPolicy 545
Menggunakan kebijakan ini 545
Rincian kebijakan 545
Versi kebijakan 545
Dokumen kebijakan JSON 545
Pelajari selengkapnya 551
AmazonEKSLocalOutpostClusterPolicy 552
Menggunakan kebijakan ini 552
Rincian kebijakan 552
Versi kebijakan 552
Dokumen kebijakan JSON 552
Pelajari selengkapnya 554
AmazonEKSLocalOutpostServiceRolePolicy 554
Menggunakan kebijakan ini 554
Rincian kebijakan 555
Versi kebijakan 555
Dokumen kebijakan JSON 555
Pelajari selengkapnya 561
AmazonEKSNetworkingPolicy 561
Menggunakan kebijakan ini 561
Rincian kebijakan 561
Versi kebijakan 561
Dokumen kebijakan JSON 562
Pelajari selengkapnya 563
AmazonEKSServicePolicy 563
Menggunakan kebijakan ini 563
Rincian kebijakan 564
Versi kebijakan 564
Dokumen kebijakan JSON 564
Pelajari selengkapnya 566
AmazonEKSServiceRolePolicy 566
Menggunakan kebijakan ini 566
Rincian kebijakan 566
Versi kebijakan 567
Dokumen kebijakan JSON 567
Pelajari selengkapnya 574

AmazonEKSVPCResourceController 575
Menggunakan kebijakan ini 575
Rincian kebijakan 575
Versi kebijakan 575
Dokumen kebijakan JSON 575
Pelajari selengkapnya 576
AmazonEKSWorkerNodeMinimalPolicy 576
Menggunakan kebijakan ini 576
Rincian kebijakan 577
Versi kebijakan 577
Dokumen kebijakan JSON 577
Pelajari selengkapnya 577
AmazonEKSWorkerNodePolicy 578
Menggunakan kebijakan ini 578
Rincian kebijakan 578
Versi kebijakan 578
Dokumen kebijakan JSON 578
Pelajari selengkapnya 579
AmazonElastiCacheFullAccess 579
Menggunakan kebijakan ini 579
Rincian kebijakan 579
Versi kebijakan 579
Dokumen kebijakan JSON 580
Pelajari selengkapnya 583
AmazonElastiCacheReadOnlyAccess 583
Menggunakan kebijakan ini 583
Rincian kebijakan 583
Versi kebijakan 584
Dokumen kebijakan JSON 584
Pelajari selengkapnya 584
AmazonElasticContainerRegistryPublicFullAccess 584
Menggunakan kebijakan ini 585
Rincian kebijakan 585
Versi kebijakan 585
Dokumen kebijakan JSON 585
Pelajari selengkapnya 586

AmazonElasticContainerRegistryPublicPowerUser 586
Menggunakan kebijakan ini 586
Rincian kebijakan 586
Versi kebijakan 586
Dokumen kebijakan JSON 587
Pelajari selengkapnya 587
AmazonElasticContainerRegistryPublicReadOnly 587
Menggunakan kebijakan ini 588
Rincian kebijakan 588
Versi kebijakan 588
Dokumen kebijakan JSON 588
Pelajari selengkapnya 589
AmazonElasticFileSystemClientFullAccess 589
Menggunakan kebijakan ini 589
Rincian kebijakan 589
Versi kebijakan 589
Dokumen kebijakan JSON 590
Pelajari selengkapnya 590
AmazonElasticFileSystemClientReadOnlyAccess 590
Menggunakan kebijakan ini 590
Rincian kebijakan 590
Versi kebijakan 591
Dokumen kebijakan JSON 591
Pelajari selengkapnya 591
AmazonElasticFileSystemClientReadWriteAccess 591
Menggunakan kebijakan ini 592
Rincian kebijakan 592
Versi kebijakan 592
Dokumen kebijakan JSON 592
Pelajari selengkapnya 593
AmazonElasticFileSystemFullAccess 593
Menggunakan kebijakan ini 593
Rincian kebijakan 593
Versi kebijakan 593
Dokumen kebijakan JSON 593
Pelajari selengkapnya 595

AmazonElasticFileSystemReadOnlyAccess 596
Menggunakan kebijakan ini 596
Rincian kebijakan 596
Versi kebijakan 596
Dokumen kebijakan JSON 596
Pelajari selengkapnya 597
AmazonElasticFileSystemServiceRolePolicy 597
Menggunakan kebijakan ini 598
Rincian kebijakan 598
Versi kebijakan 598
Dokumen kebijakan JSON 598
Pelajari selengkapnya 600
AmazonElasticFileSystemsUtils 600
Menggunakan kebijakan ini 601
Rincian kebijakan 601
Versi kebijakan 601
Dokumen kebijakan JSON 601
Pelajari selengkapnya 603
AmazonElasticMapReduceEditorsRole 603
Menggunakan kebijakan ini 603
Rincian kebijakan 603
Versi kebijakan 604
Dokumen kebijakan JSON 604
Pelajari selengkapnya 605
AmazonElasticMapReduceforAutoScalingRole 605
Menggunakan kebijakan ini 605
Rincian kebijakan 605
Versi kebijakan 606
Dokumen kebijakan JSON 606
Pelajari selengkapnya 606
AmazonElasticMapReduceforEC2Role 606
Menggunakan kebijakan ini 607
Rincian kebijakan 607
Versi kebijakan 607
Dokumen kebijakan JSON 607
Pelajari selengkapnya 609

AmazonElasticMapReduceFullAccess 609
Menggunakan kebijakan ini 609
Rincian kebijakan 609
Versi kebijakan 609
Dokumen kebijakan JSON 610
Pelajari selengkapnya 611
AmazonElasticMapReducePlacementGroupPolicy 611
Menggunakan kebijakan ini 612
Rincian kebijakan 612
Versi kebijakan 612
Dokumen kebijakan JSON 612
Pelajari selengkapnya 613
AmazonElasticMapReduceReadOnlyAccess 613
Menggunakan kebijakan ini 613
Rincian kebijakan 613
Versi kebijakan 613
Dokumen kebijakan JSON 614
Pelajari selengkapnya 614
AmazonElasticMapReduceRole 614
Menggunakan kebijakan ini 615
Rincian kebijakan 615
Versi kebijakan 615
Dokumen kebijakan JSON 615
Pelajari selengkapnya 617
AmazonElasticsearchServiceRolePolicy 617
Menggunakan kebijakan ini 618
Rincian kebijakan 618
Versi kebijakan 618
Dokumen kebijakan JSON 618
Pelajari selengkapnya 621
AmazonElasticTranscoder_FullAccess 621
Menggunakan kebijakan ini 621
Rincian kebijakan 621
Versi kebijakan 622
Dokumen kebijakan JSON 622
Pelajari selengkapnya 623

AmazonElasticTranscoder_JobsSubmitter 623
Menggunakan kebijakan ini 623
Rincian kebijakan 623
Versi kebijakan 623
Dokumen kebijakan JSON 624
Pelajari selengkapnya 624
AmazonElasticTranscoder_ReadOnlyAccess 624
Menggunakan kebijakan ini 625
Rincian kebijakan 625
Versi kebijakan 625
Dokumen kebijakan JSON 625
Pelajari selengkapnya 626
AmazonElasticTranscoderRole 626
Menggunakan kebijakan ini 626
Rincian kebijakan 626
Versi kebijakan 626
Dokumen kebijakan JSON 626
Pelajari selengkapnya 627
AmazonEMRCleanupPolicy 627
Menggunakan kebijakan ini 628
Rincian kebijakan 628
Versi kebijakan 628
Dokumen kebijakan JSON 628
Pelajari selengkapnya 629
AmazonEMRContainersServiceRolePolicy 629
Menggunakan kebijakan ini 629
Rincian kebijakan 629
Versi kebijakan 630
Dokumen kebijakan JSON 630
Pelajari selengkapnya 631
AmazonEMRFullAccessPolicy_v2 631
Menggunakan kebijakan ini 631
Rincian kebijakan 631
Versi kebijakan 632
Dokumen kebijakan JSON 632
Pelajari selengkapnya 635

AmazonEMRReadOnlyAccessPolicy_v2 635
Menggunakan kebijakan ini 636
Rincian kebijakan 636
Versi kebijakan 636
Dokumen kebijakan JSON 636
Pelajari selengkapnya 637
AmazonEMRServerlessServiceRolePolicy 637
Menggunakan kebijakan ini 638
Rincian kebijakan 638
Versi kebijakan 638
Dokumen kebijakan JSON 638
Pelajari selengkapnya 639
AmazonEMRServicePolicy_v2 639
Menggunakan kebijakan ini 639
Rincian kebijakan 640
Versi kebijakan 640
Dokumen kebijakan JSON 640
Pelajari selengkapnya 649
AmazonESCognitoAccess 649
Menggunakan kebijakan ini 649
Rincian kebijakan 649
Versi kebijakan 649
Dokumen kebijakan JSON 650
Pelajari selengkapnya 650
AmazonESFullAccess 651
Menggunakan kebijakan ini 651
Rincian kebijakan 651
Versi kebijakan 651
Dokumen kebijakan JSON 651
Pelajari selengkapnya 652
AmazonESReadOnlyAccess 652
Menggunakan kebijakan ini 652
Rincian kebijakan 652
Versi kebijakan 652
Dokumen kebijakan JSON 653
Pelajari selengkapnya 653

AmazonEventBridgeApiDestinationsServiceRolePolicy 653
Menggunakan kebijakan ini 653
Rincian kebijakan 654
Versi kebijakan 654
Dokumen kebijakan JSON 654
Pelajari selengkapnya 655
AmazonEventBridgeFullAccess 655
Menggunakan kebijakan ini 655
Rincian kebijakan 655
Versi kebijakan 656
Dokumen kebijakan JSON 656
Pelajari selengkapnya 658
AmazonEventBridgePipesFullAccess 658
Menggunakan kebijakan ini 658
Rincian kebijakan 658
Versi kebijakan 659
Dokumen kebijakan JSON 659
Pelajari selengkapnya 659
AmazonEventBridgePipesOperatorAccess 660
Menggunakan kebijakan ini 660
Rincian kebijakan 660
Versi kebijakan 660
Dokumen kebijakan JSON 660
Pelajari selengkapnya 661
AmazonEventBridgePipesReadOnlyAccess 661
Menggunakan kebijakan ini 661
Rincian kebijakan 661
Versi kebijakan 661
Dokumen kebijakan JSON 662
Pelajari selengkapnya 662
AmazonEventBridgeReadOnlyAccess 662
Menggunakan kebijakan ini 662
Rincian kebijakan 662
Versi kebijakan 663
Dokumen kebijakan JSON 663
Pelajari selengkapnya 664

AmazonEventBridgeSchedulerFullAccess 664
Menggunakan kebijakan ini 665
Rincian kebijakan 665
Versi kebijakan 665
Dokumen kebijakan JSON 665
Pelajari selengkapnya 666
AmazonEventBridgeSchedulerReadOnlyAccess 666
Menggunakan kebijakan ini 666
Rincian kebijakan 666
Versi kebijakan 666
Dokumen kebijakan JSON 667
Pelajari selengkapnya 667
AmazonEventBridgeSchemasFullAccess 667
Menggunakan kebijakan ini 667
Rincian kebijakan 668
Versi kebijakan 668
Dokumen kebijakan JSON 668
Pelajari selengkapnya 669
AmazonEventBridgeSchemasReadOnlyAccess 669
Menggunakan kebijakan ini 669
Rincian kebijakan 669
Versi kebijakan 670
Dokumen kebijakan JSON 670
Pelajari selengkapnya 670
AmazonEventBridgeSchemasServiceRolePolicy 671
Menggunakan kebijakan ini 671
Rincian kebijakan 671
Versi kebijakan 671
Dokumen kebijakan JSON 671
Pelajari selengkapnya 672
AmazonEVSServiceRolePolicy 672
Menggunakan kebijakan ini 672
Rincian kebijakan 672
Versi kebijakan 673
Dokumen kebijakan JSON 673
Pelajari selengkapnya 675

AmazonFISServiceRolePolicy 675
Menggunakan kebijakan ini 675
Rincian kebijakan 675
Versi kebijakan 675
Dokumen kebijakan JSON 676
Pelajari selengkapnya 677
AmazonForecastFullAccess 677
Menggunakan kebijakan ini 677
Rincian kebijakan 678
Versi kebijakan 678
Dokumen kebijakan JSON 678
Pelajari selengkapnya 679
AmazonFraudDetectorFullAccessPolicy 679
Menggunakan kebijakan ini 679
Rincian kebijakan 679
Versi kebijakan 679
Dokumen kebijakan JSON 680
Pelajari selengkapnya 681
AmazonFreeRTOSFullAccess 681
Menggunakan kebijakan ini 681
Rincian kebijakan 681
Versi kebijakan 681
Dokumen kebijakan JSON 682
Pelajari selengkapnya 682
AmazonFreeRTOSOTAUpdate 682
Menggunakan kebijakan ini 682
Rincian kebijakan 682
Versi kebijakan 683
Dokumen kebijakan JSON 683
Pelajari selengkapnya 684
AmazonFSxConsoleFullAccess 684
Menggunakan kebijakan ini 685
Rincian kebijakan 685
Versi kebijakan 685
Dokumen kebijakan JSON 685
Pelajari selengkapnya 689

AmazonFSxConsoleReadOnlyAccess 689
Menggunakan kebijakan ini 689
Rincian kebijakan 689
Versi kebijakan 689
Dokumen kebijakan JSON 689
Pelajari selengkapnya 690
AmazonFSxFullAccess 690
Menggunakan kebijakan ini 691
Rincian kebijakan 691
Versi kebijakan 691
Dokumen kebijakan JSON 691
Pelajari selengkapnya 695
AmazonFSxReadOnlyAccess 695
Menggunakan kebijakan ini 695
Rincian kebijakan 696
Versi kebijakan 696
Dokumen kebijakan JSON 696
Pelajari selengkapnya 696
AmazonFSxServiceRolePolicy 697
Menggunakan kebijakan ini 697
Rincian kebijakan 697
Versi kebijakan 697
Dokumen kebijakan JSON 697
Pelajari selengkapnya 700
AmazonGlacierFullAccess 700
Menggunakan kebijakan ini 700
Rincian kebijakan 700
Versi kebijakan 701
Dokumen kebijakan JSON 701
Pelajari selengkapnya 701
AmazonGlacierReadOnlyAccess 701
Menggunakan kebijakan ini 701
Rincian kebijakan 702
Versi kebijakan 702
Dokumen kebijakan JSON 702
Pelajari selengkapnya 703

AmazonGrafanaAthenaAccess 703
Menggunakan kebijakan ini 703
Rincian kebijakan 703
Versi kebijakan 703
Dokumen kebijakan JSON 703
Pelajari selengkapnya 705
AmazonGrafanaCloudWatchAccess 705
Menggunakan kebijakan ini 706
Rincian kebijakan 706
Versi kebijakan 706
Dokumen kebijakan JSON 706
Pelajari selengkapnya 707
AmazonGrafanaRedshiftAccess 708
Menggunakan kebijakan ini 708
Rincian kebijakan 708
Versi kebijakan 708
Dokumen kebijakan JSON 708
Pelajari selengkapnya 709
AmazonGrafanaServiceLinkedRolePolicy 710
Menggunakan kebijakan ini 710
Rincian kebijakan 710
Versi kebijakan 710
Dokumen kebijakan JSON 710
Pelajari selengkapnya 712
AmazonGuardDutyFullAccess 712
Menggunakan kebijakan ini 712
Rincian kebijakan 712
Versi kebijakan 712
Dokumen kebijakan JSON 712
Pelajari selengkapnya 714
AmazonGuardDutyFullAccess_v2 714
Menggunakan kebijakan ini 714
Rincian kebijakan 714
Versi kebijakan 715
Dokumen kebijakan JSON 715
Pelajari selengkapnya 717

AmazonGuardDutyMalwareProtectionServiceRolePolicy 717
Menggunakan kebijakan ini 717
Rincian kebijakan 717
Versi kebijakan 718
Dokumen kebijakan JSON 718
Pelajari selengkapnya 722
AmazonGuardDutyReadOnlyAccess 722
Menggunakan kebijakan ini 722
Rincian kebijakan 723
Versi kebijakan 723
Dokumen kebijakan JSON 723
Pelajari selengkapnya 724
AmazonGuardDutyServiceRolePolicy 724
Menggunakan kebijakan ini 724
Rincian kebijakan 724
Versi kebijakan 724
Dokumen kebijakan JSON 725
Pelajari selengkapnya 731
AmazonHealthLakeFullAccess 731
Menggunakan kebijakan ini 731
Rincian kebijakan 731
Versi kebijakan 731
Dokumen kebijakan JSON 731
Pelajari selengkapnya 732
AmazonHealthLakeReadOnlyAccess 732
Menggunakan kebijakan ini 733
Rincian kebijakan 733
Versi kebijakan 733
Dokumen kebijakan JSON 733
Pelajari selengkapnya 734
AmazonHoneycodeFullAccess 734
Menggunakan kebijakan ini 734
Rincian kebijakan 734
Versi kebijakan 734
Dokumen kebijakan JSON 734
Pelajari selengkapnya 735

AmazonHoneycodeReadOnlyAccess 735
Menggunakan kebijakan ini 735
Rincian kebijakan 735
Versi kebijakan 736
Dokumen kebijakan JSON 736
Pelajari selengkapnya 736
AmazonHoneycodeServiceRolePolicy 736
Menggunakan kebijakan ini 737
Rincian kebijakan 737
Versi kebijakan 737
Dokumen kebijakan JSON 737
Pelajari selengkapnya 738
AmazonHoneycodeTeamAssociationFullAccess 738
Menggunakan kebijakan ini 738
Rincian kebijakan 738
Versi kebijakan 738
Dokumen kebijakan JSON 738
Pelajari selengkapnya 739
AmazonHoneycodeTeamAssociationReadOnlyAccess 739
Menggunakan kebijakan ini 739
Rincian kebijakan 739
Versi kebijakan 740
Dokumen kebijakan JSON 740
Pelajari selengkapnya 740
AmazonHoneycodeWorkbookFullAccess 740
Menggunakan kebijakan ini 741
Rincian kebijakan 741
Versi kebijakan 741
Dokumen kebijakan JSON 741
Pelajari selengkapnya 742
AmazonHoneycodeWorkbookReadOnlyAccess 742
Menggunakan kebijakan ini 742
Rincian kebijakan 742
Versi kebijakan 742
Dokumen kebijakan JSON 743
Pelajari selengkapnya 743

AmazonInspector2AgentlessServiceRolePolicy 743
Menggunakan kebijakan ini 744
Rincian kebijakan 744
Versi kebijakan 744
Dokumen kebijakan JSON 744
Pelajari selengkapnya 748
AmazonInspector2FullAccess 748
Menggunakan kebijakan ini 748
Rincian kebijakan 748
Versi kebijakan 748
Dokumen kebijakan JSON 749
Pelajari selengkapnya 750
AmazonInspector2FullAccess_v2 750
Menggunakan kebijakan ini 750
Rincian kebijakan 750
Versi kebijakan 750
Dokumen kebijakan JSON 751
Pelajari selengkapnya 753
AmazonInspector2ManagedCisPolicy 753
Menggunakan kebijakan ini 753
Rincian kebijakan 753
Versi kebijakan 753
Dokumen kebijakan JSON 753
Pelajari selengkapnya 754
AmazonInspector2ReadOnlyAccess 754
Menggunakan kebijakan ini 754
Rincian kebijakan 754
Versi kebijakan 755
Dokumen kebijakan JSON 755
Pelajari selengkapnya 755
AmazonInspector2ServiceRolePolicy 756
Menggunakan kebijakan ini 756
Rincian kebijakan 756
Versi kebijakan 756
Dokumen kebijakan JSON 756
Pelajari selengkapnya 764

AmazonInspectorFullAccess 764
Menggunakan kebijakan ini 764
Rincian kebijakan 764
Versi kebijakan 764
Dokumen kebijakan JSON 765
Pelajari selengkapnya 766
AmazonInspectorReadOnlyAccess 766
Menggunakan kebijakan ini 766
Rincian kebijakan 766
Versi kebijakan 766
Dokumen kebijakan JSON 767
Pelajari selengkapnya 767
AmazonInspectorServiceRolePolicy 767
Menggunakan kebijakan ini 768
Rincian kebijakan 768
Versi kebijakan 768
Dokumen kebijakan JSON 768
Pelajari selengkapnya 769
AmazonKendraFullAccess 770
Menggunakan kebijakan ini 770
Rincian kebijakan 770
Versi kebijakan 770
Dokumen kebijakan JSON 770
Pelajari selengkapnya 772
AmazonKendraReadOnlyAccess 772
Menggunakan kebijakan ini 772
Rincian kebijakan 772
Versi kebijakan 773
Dokumen kebijakan JSON 773
Pelajari selengkapnya 773
AmazonKeyspacesFullAccess 774
Menggunakan kebijakan ini 774
Rincian kebijakan 774
Versi kebijakan 774
Dokumen kebijakan JSON 774
Pelajari selengkapnya 776

AmazonKeyspacesReadOnlyAccess 777
Menggunakan kebijakan ini 777
Rincian kebijakan 777
Versi kebijakan 777
Dokumen kebijakan JSON 777
Pelajari selengkapnya 778
AmazonKeyspacesReadOnlyAccess_v2 778
Menggunakan kebijakan ini 778
Rincian kebijakan 778
Versi kebijakan 779
Dokumen kebijakan JSON 779
Pelajari selengkapnya 780
AmazonKinesisAnalyticsFullAccess 780
Menggunakan kebijakan ini 780
Rincian kebijakan 780
Versi kebijakan 781
Dokumen kebijakan JSON 781
Pelajari selengkapnya 782
AmazonKinesisAnalyticsReadOnly 782
Menggunakan kebijakan ini 783
Rincian kebijakan 783
Versi kebijakan 783
Dokumen kebijakan JSON 783
Pelajari selengkapnya 784
AmazonKinesisFirehoseFullAccess 785
Menggunakan kebijakan ini 785
Rincian kebijakan 785
Versi kebijakan 785
Dokumen kebijakan JSON 785
Pelajari selengkapnya 786
AmazonKinesisFirehoseReadOnlyAccess 786
Menggunakan kebijakan ini 786
Rincian kebijakan 786
Versi kebijakan 786
Dokumen kebijakan JSON 787
Pelajari selengkapnya 787

AmazonKinesisFullAccess 787
Menggunakan kebijakan ini 787
Rincian kebijakan 787
Versi kebijakan 788
Dokumen kebijakan JSON 788
Pelajari selengkapnya 788
AmazonKinesisReadOnlyAccess 788
Menggunakan kebijakan ini 788
Rincian kebijakan 789
Versi kebijakan 789
Dokumen kebijakan JSON 789
Pelajari selengkapnya 789
AmazonKinesisVideoStreamsFullAccess 790
Menggunakan kebijakan ini 790
Rincian kebijakan 790
Versi kebijakan 790
Dokumen kebijakan JSON 790
Pelajari selengkapnya 791
AmazonKinesisVideoStreamsReadOnlyAccess 791
Menggunakan kebijakan ini 791
Rincian kebijakan 791
Versi kebijakan 791
Dokumen kebijakan JSON 791
Pelajari selengkapnya 792
AmazonLaunchWizard_Fullaccess 792
Menggunakan kebijakan ini 792
Rincian kebijakan 792
Versi kebijakan 793
Dokumen kebijakan JSON 793
Pelajari selengkapnya 807
AmazonLaunchWizardFullAccessV2 807
Menggunakan kebijakan ini 807
Rincian kebijakan 807
Versi kebijakan 808
Dokumen kebijakan JSON 808
Pelajari selengkapnya 824

AmazonLexChannelsAccess 824
Menggunakan kebijakan ini 825
Rincian kebijakan 825
Versi kebijakan 825
Dokumen kebijakan JSON 825
Pelajari selengkapnya 825
AmazonLexFullAccess 826
Menggunakan kebijakan ini 826
Rincian kebijakan 826
Versi kebijakan 826
Dokumen kebijakan JSON 826
Pelajari selengkapnya 832
AmazonLexReadOnly 832
Menggunakan kebijakan ini 832
Rincian kebijakan 832
Versi kebijakan 832
Dokumen kebijakan JSON 833
Pelajari selengkapnya 834
AmazonLexReplicationPolicy 834
Menggunakan kebijakan ini 835
Rincian kebijakan 835
Versi kebijakan 835
Dokumen kebijakan JSON 835
Pelajari selengkapnya 837
AmazonLexRunBotsOnly 838
Menggunakan kebijakan ini 838
Rincian kebijakan 838
Versi kebijakan 838
Dokumen kebijakan JSON 838
Pelajari selengkapnya 839
AmazonLexV2BotPolicy 839
Menggunakan kebijakan ini 839
Rincian kebijakan 839
Versi kebijakan 839
Dokumen kebijakan JSON 840
Pelajari selengkapnya 840

AmazonLookoutEquipmentFullAccess 840
Menggunakan kebijakan ini 840
Rincian kebijakan 840
Versi kebijakan 841
Dokumen kebijakan JSON 841
Pelajari selengkapnya 842
AmazonLookoutEquipmentReadOnlyAccess 842
Menggunakan kebijakan ini 842
Rincian kebijakan 843
Versi kebijakan 843
Dokumen kebijakan JSON 843
Pelajari selengkapnya 843
AmazonLookoutMetricsFullAccess 844
Menggunakan kebijakan ini 844
Rincian kebijakan 844
Versi kebijakan 844
Dokumen kebijakan JSON 844
Pelajari selengkapnya 845
AmazonLookoutMetricsReadOnlyAccess 845
Menggunakan kebijakan ini 845
Rincian kebijakan 845
Versi kebijakan 846
Dokumen kebijakan JSON 846
Pelajari selengkapnya 846
AmazonLookoutVisionConsoleFullAccess 847
Menggunakan kebijakan ini 847
Rincian kebijakan 847
Versi kebijakan 847
Dokumen kebijakan JSON 847
Pelajari selengkapnya 850
AmazonLookoutVisionConsoleReadOnlyAccess 850
Menggunakan kebijakan ini 850
Rincian kebijakan 850
Versi kebijakan 850
Dokumen kebijakan JSON 850
Pelajari selengkapnya 852

AmazonLookoutVisionFullAccess 852
Menggunakan kebijakan ini 852
Rincian kebijakan 852
Versi kebijakan 852
Dokumen kebijakan JSON 853
Pelajari selengkapnya 853
AmazonLookoutVisionReadOnlyAccess 853
Menggunakan kebijakan ini 853
Rincian kebijakan 854
Versi kebijakan 854
Dokumen kebijakan JSON 854
Pelajari selengkapnya 855
AmazonMachineLearningBatchPredictionsAccess 855
Menggunakan kebijakan ini 855
Rincian kebijakan 855
Versi kebijakan 855
Dokumen kebijakan JSON 855
Pelajari selengkapnya 856
AmazonMachineLearningCreateOnlyAccess 856
Menggunakan kebijakan ini 856
Rincian kebijakan 856
Versi kebijakan 857
Dokumen kebijakan JSON 857
Pelajari selengkapnya 857
AmazonMachineLearningFullAccess 857
Menggunakan kebijakan ini 858
Rincian kebijakan 858
Versi kebijakan 858
Dokumen kebijakan JSON 858
Pelajari selengkapnya 859
AmazonMachineLearningManageRealTimeEndpointOnlyAccess 859
Menggunakan kebijakan ini 859
Rincian kebijakan 859
Versi kebijakan 859
Dokumen kebijakan JSON 860
Pelajari selengkapnya 860

AmazonMachineLearningReadOnlyAccess 860
Menggunakan kebijakan ini 860
Rincian kebijakan 860
Versi kebijakan 861
Dokumen kebijakan JSON 861
Pelajari selengkapnya 861
AmazonMachineLearningRealTimePredictionOnlyAccess 861
Menggunakan kebijakan ini 862
Rincian kebijakan 862
Versi kebijakan 862
Dokumen kebijakan JSON 862
Pelajari selengkapnya 863
AmazonMachineLearningRoleforRedshiftDataSourceV3 863
Menggunakan kebijakan ini 863
Rincian kebijakan 863
Versi kebijakan 863
Dokumen kebijakan JSON 864
Pelajari selengkapnya 864
AmazonMacieFullAccess 865
Menggunakan kebijakan ini 865
Rincian kebijakan 865
Versi kebijakan 865
Dokumen kebijakan JSON 865
Pelajari selengkapnya 866
AmazonMacieHandshakeRole 866
Menggunakan kebijakan ini 866
Rincian kebijakan 866
Versi kebijakan 867
Dokumen kebijakan JSON 867
Pelajari selengkapnya 867
AmazonMacieReadOnlyAccess 868
Menggunakan kebijakan ini 868
Rincian kebijakan 868
Versi kebijakan 868
Dokumen kebijakan JSON 868
Pelajari selengkapnya 869

AmazonMacieServiceRole 869
Menggunakan kebijakan ini 869
Rincian kebijakan 869
Versi kebijakan 869
Dokumen kebijakan JSON 870
Pelajari selengkapnya 870
AmazonMacieServiceRolePolicy 870
Menggunakan kebijakan ini 870
Rincian kebijakan 870
Versi kebijakan 871
Dokumen kebijakan JSON 871
Pelajari selengkapnya 872
AmazonManagedBlockchainConsoleFullAccess 872
Menggunakan kebijakan ini 873
Rincian kebijakan 873
Versi kebijakan 873
Dokumen kebijakan JSON 873
Pelajari selengkapnya 874
AmazonManagedBlockchainFullAccess 874
Menggunakan kebijakan ini 874
Rincian kebijakan 874
Versi kebijakan 874
Dokumen kebijakan JSON 875
Pelajari selengkapnya 875
AmazonManagedBlockchainReadOnlyAccess 875
Menggunakan kebijakan ini 875
Rincian kebijakan 875
Versi kebijakan 876
Dokumen kebijakan JSON 876
Pelajari selengkapnya 876
AmazonManagedBlockchainServiceRolePolicy 877
Menggunakan kebijakan ini 877
Rincian kebijakan 877
Versi kebijakan 877
Dokumen kebijakan JSON 877
Pelajari selengkapnya 878

AmazonMCSFullAccess 878
Menggunakan kebijakan ini 878
Rincian kebijakan 878
Versi kebijakan 879
Dokumen kebijakan JSON 879
Pelajari selengkapnya 880
AmazonMCSReadOnlyAccess 880
Menggunakan kebijakan ini 880
Rincian kebijakan 880
Versi kebijakan 881
Dokumen kebijakan JSON 881
Pelajari selengkapnya 881
AmazonMechanicalTurkFullAccess 882
Menggunakan kebijakan ini 882
Rincian kebijakan 882
Versi kebijakan 882
Dokumen kebijakan JSON 882
Pelajari selengkapnya 883
AmazonMechanicalTurkReadOnly 883
Menggunakan kebijakan ini 883
Rincian kebijakan 883
Versi kebijakan 883
Dokumen kebijakan JSON 884
Pelajari selengkapnya 884
AmazonMemoryDBFullAccess 884
Menggunakan kebijakan ini 884
Rincian kebijakan 884
Versi kebijakan 885
Dokumen kebijakan JSON 885
Pelajari selengkapnya 885
AmazonMemoryDBReadOnlyAccess 886
Menggunakan kebijakan ini 886
Rincian kebijakan 886
Versi kebijakan 886
Dokumen kebijakan JSON 886
Pelajari selengkapnya 887

AmazonMobileAnalyticsFinancialReportAccess 887
Menggunakan kebijakan ini 887
Rincian kebijakan 887
Versi kebijakan 887
Dokumen kebijakan JSON 888
Pelajari selengkapnya 888
AmazonMobileAnalyticsFullAccess 888
Menggunakan kebijakan ini 888
Rincian kebijakan 889
Versi kebijakan 889
Dokumen kebijakan JSON 889
Pelajari selengkapnya 889
AmazonMobileAnalyticsNon-financialReportAccess 890
Menggunakan kebijakan ini 890
Rincian kebijakan 890
Versi kebijakan 890
Dokumen kebijakan JSON 890
Pelajari selengkapnya 891
AmazonMobileAnalyticsWriteOnlyAccess 891
Menggunakan kebijakan ini 891
Rincian kebijakan 891
Versi kebijakan 891
Dokumen kebijakan JSON 892
Pelajari selengkapnya 892
AmazonMonitronFullAccess 892
Menggunakan kebijakan ini 892
Rincian kebijakan 892
Versi kebijakan 893
Dokumen kebijakan JSON 893
Pelajari selengkapnya 895
AmazonMQApiFullAccess 895
Menggunakan kebijakan ini 895
Rincian kebijakan 895
Versi kebijakan 895
Dokumen kebijakan JSON 895
Pelajari selengkapnya 896

AmazonMQApiReadOnlyAccess 897
Menggunakan kebijakan ini 897
Rincian kebijakan 897
Versi kebijakan 897
Dokumen kebijakan JSON 897
Pelajari selengkapnya 898
AmazonMQFullAccess 898
Menggunakan kebijakan ini 898
Rincian kebijakan 898
Versi kebijakan 898
Dokumen kebijakan JSON 899
Pelajari selengkapnya 900
AmazonMQReadOnlyAccess 900
Menggunakan kebijakan ini 900
Rincian kebijakan 900
Versi kebijakan 900
Dokumen kebijakan JSON 901
Pelajari selengkapnya 901
AmazonMQServiceRolePolicy 901
Menggunakan kebijakan ini 902
Rincian kebijakan 902
Versi kebijakan 902
Dokumen kebijakan JSON 902
Pelajari selengkapnya 904
AmazonMSKConnectReadOnlyAccess 904
Menggunakan kebijakan ini 904
Rincian kebijakan 904
Versi kebijakan 905
Dokumen kebijakan JSON 905
Pelajari selengkapnya 906
AmazonMSKFullAccess 906
Menggunakan kebijakan ini 906
Rincian kebijakan 906
Versi kebijakan 906
Dokumen kebijakan JSON 907
Pelajari selengkapnya 909

AmazonMSKReadOnlyAccess 910
Menggunakan kebijakan ini 910
Rincian kebijakan 910
Versi kebijakan 910
Dokumen kebijakan JSON 910
Pelajari selengkapnya 911
AmazonMWAAServiceRolePolicy 911
Menggunakan kebijakan ini 911
Rincian kebijakan 911
Versi kebijakan 912
Dokumen kebijakan JSON 912
Pelajari selengkapnya 914
AmazonNimbleStudio-LaunchProfileWorker 914
Menggunakan kebijakan ini 914
Rincian kebijakan 914
Versi kebijakan 915
Dokumen kebijakan JSON 915
Pelajari selengkapnya 915
AmazonNimbleStudio-StudioAdmin 916
Menggunakan kebijakan ini 916
Rincian kebijakan 916
Versi kebijakan 916
Dokumen kebijakan JSON 916
Pelajari selengkapnya 918
AmazonNimbleStudio-StudioUser 918
Menggunakan kebijakan ini 919
Rincian kebijakan 919
Versi kebijakan 919
Dokumen kebijakan JSON 919
Pelajari selengkapnya 921
AmazonODBServiceRolePolicy 921
Menggunakan kebijakan ini 922
Rincian kebijakan 922
Versi kebijakan 922
Dokumen kebijakan JSON 922
Pelajari selengkapnya 923

AmazonOmicsFullAccess 924
Menggunakan kebijakan ini 924
Rincian kebijakan 924
Versi kebijakan 924
Dokumen kebijakan JSON 924
Pelajari selengkapnya 925
AmazonOmicsReadOnlyAccess 925
Menggunakan kebijakan ini 925
Rincian kebijakan 926
Versi kebijakan 926
Dokumen kebijakan JSON 926
Pelajari selengkapnya 926
AmazonOneEnterpriseFullAccess 927
Menggunakan kebijakan ini 927
Rincian kebijakan 927
Versi kebijakan 927
Dokumen kebijakan JSON 927
Pelajari selengkapnya 928
AmazonOneEnterpriseInstallerAccess 928
Menggunakan kebijakan ini 928
Rincian kebijakan 928
Versi kebijakan 928
Dokumen kebijakan JSON 929
Pelajari selengkapnya 929
AmazonOneEnterpriseReadOnlyAccess 929
Menggunakan kebijakan ini 929
Rincian kebijakan 930
Versi kebijakan 930
Dokumen kebijakan JSON 930
Pelajari selengkapnya 930
AmazonOpenSearchDashboardsServiceRolePolicy 931
Menggunakan kebijakan ini 931
Rincian kebijakan 931
Versi kebijakan 931
Dokumen kebijakan JSON 931
Pelajari selengkapnya 932

AmazonOpenSearchDirectQueryGlueCreateAccess 932
Menggunakan kebijakan ini 932
Rincian kebijakan 932
Versi kebijakan 932
Dokumen kebijakan JSON 933
Pelajari selengkapnya 933
AmazonOpenSearchIngestionFullAccess 933
Menggunakan kebijakan ini 934
Rincian kebijakan 934
Versi kebijakan 934
Dokumen kebijakan JSON 934
Pelajari selengkapnya 935
AmazonOpenSearchIngestionReadOnlyAccess 935
Menggunakan kebijakan ini 935
Rincian kebijakan 935
Versi kebijakan 936
Dokumen kebijakan JSON 936
Pelajari selengkapnya 936
AmazonOpenSearchIngestionServiceRolePolicy 937
Menggunakan kebijakan ini 937
Rincian kebijakan 937
Versi kebijakan 937
Dokumen kebijakan JSON 937
Pelajari selengkapnya 939
AmazonOpenSearchServerlessServiceRolePolicy 939
Menggunakan kebijakan ini 939
Rincian kebijakan 940
Versi kebijakan 940
Dokumen kebijakan JSON 940
Pelajari selengkapnya 940
AmazonOpenSearchServiceCognitoAccess 941
Menggunakan kebijakan ini 941
Rincian kebijakan 941
Versi kebijakan 941
Dokumen kebijakan JSON 941
Pelajari selengkapnya 942

AmazonOpenSearchServiceFullAccess 943
Menggunakan kebijakan ini 943
Rincian kebijakan 943
Versi kebijakan 943
Dokumen kebijakan JSON 943
Pelajari selengkapnya 944
AmazonOpenSearchServiceReadOnlyAccess 944
Menggunakan kebijakan ini 944
Rincian kebijakan 944
Versi kebijakan 944
Dokumen kebijakan JSON 945
Pelajari selengkapnya 945
AmazonOpenSearchServiceRolePolicy 945
Menggunakan kebijakan ini 945
Rincian kebijakan 946
Versi kebijakan 946
Dokumen kebijakan JSON 946
Pelajari selengkapnya 951
AmazonPersonalizeFullAccess 951
Menggunakan kebijakan ini 951
Rincian kebijakan 951
Versi kebijakan 951
Dokumen kebijakan JSON 952
Pelajari selengkapnya 953
AmazonPollyFullAccess 953
Menggunakan kebijakan ini 953
Rincian kebijakan 953
Versi kebijakan 953
Dokumen kebijakan JSON 954
Pelajari selengkapnya 954
AmazonPollyReadOnlyAccess 954
Menggunakan kebijakan ini 954
Rincian kebijakan 955
Versi kebijakan 955
Dokumen kebijakan JSON 955
Pelajari selengkapnya 955

AmazonPrometheusConsoleFullAccess 956
Menggunakan kebijakan ini 956
Rincian kebijakan 956
Versi kebijakan 956
Dokumen kebijakan JSON 956
Pelajari selengkapnya 957
AmazonPrometheusFullAccess 958
Menggunakan kebijakan ini 958
Rincian kebijakan 958
Versi kebijakan 958
Dokumen kebijakan JSON 958
Pelajari selengkapnya 959
AmazonPrometheusQueryAccess 960
Menggunakan kebijakan ini 960
Rincian kebijakan 960
Versi kebijakan 960
Dokumen kebijakan JSON 960
Pelajari selengkapnya 961
AmazonPrometheusRemoteWriteAccess 961
Menggunakan kebijakan ini 961
Rincian kebijakan 961
Versi kebijakan 961
Dokumen kebijakan JSON 962
Pelajari selengkapnya 962
AmazonPrometheusScraperServiceRolePolicy 962
Menggunakan kebijakan ini 962
Rincian kebijakan 962
Versi kebijakan 963
Dokumen kebijakan JSON 963
Pelajari selengkapnya 965
AmazonQDeveloperAccess 965
Menggunakan kebijakan ini 965
Rincian kebijakan 966
Versi kebijakan 966
Dokumen kebijakan JSON 966
Pelajari selengkapnya 967

AmazonQFullAccess 967
Menggunakan kebijakan ini 967
Rincian kebijakan 968
Versi kebijakan 968
Dokumen kebijakan JSON 968
Pelajari selengkapnya 970
AmazonQLDBConsoleFullAccess 970
Menggunakan kebijakan ini 970
Rincian kebijakan 970
Versi kebijakan 970
Dokumen kebijakan JSON 971
Pelajari selengkapnya 972
AmazonQLDBFullAccess 972
Menggunakan kebijakan ini 973
Rincian kebijakan 973
Versi kebijakan 973
Dokumen kebijakan JSON 973
Pelajari selengkapnya 974
AmazonQLDBReadOnly 975
Menggunakan kebijakan ini 975
Rincian kebijakan 975
Versi kebijakan 975
Dokumen kebijakan JSON 975
Pelajari selengkapnya 976
AmazonRDSBetaServiceRolePolicy 976
Menggunakan kebijakan ini 976
Rincian kebijakan 976
Versi kebijakan 977
Dokumen kebijakan JSON 977
Pelajari selengkapnya 980
AmazonRDSCustomInstanceProfileRolePolicy 980
Menggunakan kebijakan ini 980
Rincian kebijakan 980
Versi kebijakan 980
Dokumen kebijakan JSON 981
Pelajari selengkapnya 988

AmazonRDSCustomPreviewServiceRolePolicy 988
Menggunakan kebijakan ini 988
Rincian kebijakan 988
Versi kebijakan 989
Dokumen kebijakan JSON 989
Pelajari selengkapnya 1006
AmazonRDSCustomServiceRolePolicy 1006
Menggunakan kebijakan ini 1006
Rincian kebijakan 1006
Versi kebijakan 1006
Dokumen kebijakan JSON 1007
Pelajari selengkapnya 1025
AmazonRDSDataFullAccess 1025
Menggunakan kebijakan ini 1025
Rincian kebijakan 1025
Versi kebijakan 1026
Dokumen kebijakan JSON 1026
Pelajari selengkapnya 1027
AmazonRDSDirectoryServiceAccess 1027
Menggunakan kebijakan ini 1027
Rincian kebijakan 1027
Versi kebijakan 1028
Dokumen kebijakan JSON 1028
Pelajari selengkapnya 1028
AmazonRDSEnhancedMonitoringRole 1028
Menggunakan kebijakan ini 1029
Rincian kebijakan 1029
Versi kebijakan 1029
Dokumen kebijakan JSON 1029
Pelajari selengkapnya 1030
AmazonRDSFullAccess 1030
Menggunakan kebijakan ini 1030
Rincian kebijakan 1030
Versi kebijakan 1031
Dokumen kebijakan JSON 1031
Pelajari selengkapnya 1033

AmazonRDSPerformanceInsightsFullAccess 1033
Menggunakan kebijakan ini 1033
Rincian kebijakan 1033
Versi kebijakan 1033
Dokumen kebijakan JSON 1034
Pelajari selengkapnya 1035
AmazonRDSPerformanceInsightsReadOnly 1035
Menggunakan kebijakan ini 1035
Rincian kebijakan 1036
Versi kebijakan 1036
Dokumen kebijakan JSON 1036
Pelajari selengkapnya 1038
AmazonRDSPreviewServiceRolePolicy 1038
Menggunakan kebijakan ini 1038
Rincian kebijakan 1038
Versi kebijakan 1038
Dokumen kebijakan JSON 1039
Pelajari selengkapnya 1042
AmazonRDSReadOnlyAccess 1042
Menggunakan kebijakan ini 1042
Rincian kebijakan 1042
Versi kebijakan 1042
Dokumen kebijakan JSON 1042
Pelajari selengkapnya 1044
AmazonRDSServiceRolePolicy 1044
Menggunakan kebijakan ini 1044
Rincian kebijakan 1044
Versi kebijakan 1044
Dokumen kebijakan JSON 1045
Pelajari selengkapnya 1048
AmazonRedshiftAllCommandsFullAccess 1048
Menggunakan kebijakan ini 1049
Rincian kebijakan 1049
Versi kebijakan 1049
Dokumen kebijakan JSON 1049
Pelajari selengkapnya 1054

AmazonRedshiftDataFullAccess 1055
Menggunakan kebijakan ini 1055
Rincian kebijakan 1055
Versi kebijakan 1055
Dokumen kebijakan JSON 1055
Pelajari selengkapnya 1057
AmazonRedshiftFullAccess 1057
Menggunakan kebijakan ini 1058
Rincian kebijakan 1058
Versi kebijakan 1058
Dokumen kebijakan JSON 1058
Pelajari selengkapnya 1060
AmazonRedshiftQueryEditor 1060
Menggunakan kebijakan ini 1060
Rincian kebijakan 1061
Versi kebijakan 1061
Dokumen kebijakan JSON 1061
Pelajari selengkapnya 1063
AmazonRedshiftQueryEditorV2FullAccess 1063
Menggunakan kebijakan ini 1063
Rincian kebijakan 1063
Versi kebijakan 1064
Dokumen kebijakan JSON 1064
Pelajari selengkapnya 1065
AmazonRedshiftQueryEditorV2NoSharing 1065
Menggunakan kebijakan ini 1066
Rincian kebijakan 1066
Versi kebijakan 1066
Dokumen kebijakan JSON 1066
Pelajari selengkapnya 1070
AmazonRedshiftQueryEditorV2ReadSharing 1070
Menggunakan kebijakan ini 1070
Rincian kebijakan 1070
Versi kebijakan 1071
Dokumen kebijakan JSON 1071
Pelajari selengkapnya 1076

AmazonRedshiftQueryEditorV2ReadWriteSharing 1076
Menggunakan kebijakan ini 1076
Rincian kebijakan 1076
Versi kebijakan 1076
Dokumen kebijakan JSON 1077
Pelajari selengkapnya 1082
AmazonRedshiftReadOnlyAccess 1082
Menggunakan kebijakan ini 1082
Rincian kebijakan 1082
Versi kebijakan 1082
Dokumen kebijakan JSON 1082
Pelajari selengkapnya 1083
AmazonRedshiftServiceLinkedRolePolicy 1083
Menggunakan kebijakan ini 1084
Rincian kebijakan 1084
Versi kebijakan 1084
Dokumen kebijakan JSON 1084
Pelajari selengkapnya 1090
AmazonRekognitionCustomLabelsFullAccess 1091
Menggunakan kebijakan ini 1091
Rincian kebijakan 1091
Versi kebijakan 1091
Dokumen kebijakan JSON 1091
Pelajari selengkapnya 1092
AmazonRekognitionFullAccess 1093
Menggunakan kebijakan ini 1093
Rincian kebijakan 1093
Versi kebijakan 1093
Dokumen kebijakan JSON 1093
Pelajari selengkapnya 1094
AmazonRekognitionReadOnlyAccess 1094
Menggunakan kebijakan ini 1094
Rincian kebijakan 1094
Versi kebijakan 1094
Dokumen kebijakan JSON 1095
Pelajari selengkapnya 1096

AmazonRekognitionServiceRole 1096
Menggunakan kebijakan ini 1096
Rincian kebijakan 1096
Versi kebijakan 1096
Dokumen kebijakan JSON 1097
Pelajari selengkapnya 1097
AmazonRoute53AutoNamingFullAccess 1098
Menggunakan kebijakan ini 1098
Rincian kebijakan 1098
Versi kebijakan 1098
Dokumen kebijakan JSON 1098
Pelajari selengkapnya 1099
AmazonRoute53AutoNamingReadOnlyAccess 1099
Menggunakan kebijakan ini 1099
Rincian kebijakan 1099
Versi kebijakan 1100
Dokumen kebijakan JSON 1100
Pelajari selengkapnya 1100
AmazonRoute53AutoNamingRegistrantAccess 1100
Menggunakan kebijakan ini 1101
Rincian kebijakan 1101
Versi kebijakan 1101
Dokumen kebijakan JSON 1101
Pelajari selengkapnya 1102
AmazonRoute53DomainsFullAccess 1102
Menggunakan kebijakan ini 1102
Rincian kebijakan 1102
Versi kebijakan 1102
Dokumen kebijakan JSON 1103
Pelajari selengkapnya 1103
AmazonRoute53DomainsReadOnlyAccess 1103
Menggunakan kebijakan ini 1103
Rincian kebijakan 1104
Versi kebijakan 1104
Dokumen kebijakan JSON 1104
Pelajari selengkapnya 1104

AmazonRoute53FullAccess 1105
Menggunakan kebijakan ini 1105
Rincian kebijakan 1105
Versi kebijakan 1105
Dokumen kebijakan JSON 1105
Pelajari selengkapnya 1106
AmazonRoute53ProfilesFullAccess 1106
Menggunakan kebijakan ini 1107
Rincian kebijakan 1107
Versi kebijakan 1107
Dokumen kebijakan JSON 1107
Pelajari selengkapnya 1108
AmazonRoute53ProfilesReadOnlyAccess 1108
Menggunakan kebijakan ini 1109
Rincian kebijakan 1109
Versi kebijakan 1109
Dokumen kebijakan JSON 1109
Pelajari selengkapnya 1110
AmazonRoute53ReadOnlyAccess 1110
Menggunakan kebijakan ini 1110
Rincian kebijakan 1110
Versi kebijakan 1110
Dokumen kebijakan JSON 1111
Pelajari selengkapnya 1111
AmazonRoute53RecoveryClusterFullAccess 1111
Menggunakan kebijakan ini 1112
Rincian kebijakan 1112
Versi kebijakan 1112
Dokumen kebijakan JSON 1112
Pelajari selengkapnya 1112
AmazonRoute53RecoveryClusterReadOnlyAccess 1113
Menggunakan kebijakan ini 1113
Rincian kebijakan 1113
Versi kebijakan 1113
Dokumen kebijakan JSON 1113
Pelajari selengkapnya 1114

AmazonRoute53RecoveryControlConfigFullAccess 1114
Menggunakan kebijakan ini 1114
Rincian kebijakan 1114
Versi kebijakan 1114
Dokumen kebijakan JSON 1115
Pelajari selengkapnya 1115
AmazonRoute53RecoveryControlConfigReadOnlyAccess 1115
Menggunakan kebijakan ini 1115
Rincian kebijakan 1115
Versi kebijakan 1116
Dokumen kebijakan JSON 1116
Pelajari selengkapnya 1116
AmazonRoute53RecoveryReadinessFullAccess 1117
Menggunakan kebijakan ini 1117
Rincian kebijakan 1117
Versi kebijakan 1117
Dokumen kebijakan JSON 1117
Pelajari selengkapnya 1118
AmazonRoute53RecoveryReadinessReadOnlyAccess 1118
Menggunakan kebijakan ini 1118
Rincian kebijakan 1118
Versi kebijakan 1118
Dokumen kebijakan JSON 1119
Pelajari selengkapnya 1120
AmazonRoute53ResolverFullAccess 1120
Menggunakan kebijakan ini 1120
Rincian kebijakan 1120
Versi kebijakan 1120
Dokumen kebijakan JSON 1120
Pelajari selengkapnya 1121
AmazonRoute53ResolverReadOnlyAccess 1121
Menggunakan kebijakan ini 1121
Rincian kebijakan 1122
Versi kebijakan 1122
Dokumen kebijakan JSON 1122
Pelajari selengkapnya 1123

AmazonS3FullAccess 1123
Menggunakan kebijakan ini 1123
Rincian kebijakan 1123
Versi kebijakan 1123
Dokumen kebijakan JSON 1123
Pelajari selengkapnya 1124
AmazonS3ObjectLambdaExecutionRolePolicy 1124
Menggunakan kebijakan ini 1124
Rincian kebijakan 1124
Versi kebijakan 1125
Dokumen kebijakan JSON 1125
Pelajari selengkapnya 1125
AmazonS3OutpostsFullAccess 1125
Menggunakan kebijakan ini 1126
Rincian kebijakan 1126
Versi kebijakan 1126
Dokumen kebijakan JSON 1126
Pelajari selengkapnya 1127
AmazonS3OutpostsReadOnlyAccess 1127
Menggunakan kebijakan ini 1127
Rincian kebijakan 1128
Versi kebijakan 1128
Dokumen kebijakan JSON 1128
Pelajari selengkapnya 1129
AmazonS3ReadOnlyAccess 1129
Menggunakan kebijakan ini 1129
Rincian kebijakan 1129
Versi kebijakan 1130
Dokumen kebijakan JSON 1130
Pelajari selengkapnya 1130
AmazonS3TablesFullAccess 1131
Menggunakan kebijakan ini 1131
Rincian kebijakan 1131
Versi kebijakan 1131
Dokumen kebijakan JSON 1131
Pelajari selengkapnya 1132

AmazonS3TablesLakeFormationServiceRole 1132
Menggunakan kebijakan ini 1132
Rincian kebijakan 1132
Versi kebijakan 1132
Dokumen kebijakan JSON 1133
Pelajari selengkapnya 1135
AmazonS3TablesReadOnlyAccess 1135
Menggunakan kebijakan ini 1135
Rincian kebijakan 1135
Versi kebijakan 1135
Dokumen kebijakan JSON 1136
Pelajari selengkapnya 1136
AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy 1136
Menggunakan kebijakan ini 1136
Rincian kebijakan 1137
Versi kebijakan 1137
Dokumen kebijakan JSON 1137
Pelajari selengkapnya 1148
AmazonSageMakerCanvasAIServicesAccess 1149
Menggunakan kebijakan ini 1149
Rincian kebijakan 1149
Versi kebijakan 1149
Dokumen kebijakan JSON 1149
Pelajari selengkapnya 1152
AmazonSageMakerCanvasBedrockAccess 1153
Menggunakan kebijakan ini 1153
Rincian kebijakan 1153
Versi kebijakan 1153
Dokumen kebijakan JSON 1153
Pelajari selengkapnya 1154
AmazonSageMakerCanvasDataPrepFullAccess 1154
Menggunakan kebijakan ini 1154
Rincian kebijakan 1155
Versi kebijakan 1155
Dokumen kebijakan JSON 1155
Pelajari selengkapnya 1164

AmazonSageMakerCanvasDirectDeployAccess 1165
Menggunakan kebijakan ini 1165
Rincian kebijakan 1165
Versi kebijakan 1165
Dokumen kebijakan JSON 1165
Pelajari selengkapnya 1166
AmazonSageMakerCanvasEMRServerlessExecutionRolePolicy 1166
Menggunakan kebijakan ini 1166
Rincian kebijakan 1167
Versi kebijakan 1167
Dokumen kebijakan JSON 1167
Pelajari selengkapnya 1168
AmazonSageMakerCanvasForecastAccess 1169
Menggunakan kebijakan ini 1169
Rincian kebijakan 1169
Versi kebijakan 1169
Dokumen kebijakan JSON 1169
Pelajari selengkapnya 1170
AmazonSageMakerCanvasFullAccess 1170
Menggunakan kebijakan ini 1170
Rincian kebijakan 1171
Versi kebijakan 1171
Dokumen kebijakan JSON 1171
Pelajari selengkapnya 1183
AmazonSageMakerCanvasSMDataScienceAssistantAccess 1183
Menggunakan kebijakan ini 1184
Rincian kebijakan 1184
Versi kebijakan 1184
Dokumen kebijakan JSON 1184
Pelajari selengkapnya 1185
AmazonSageMakerClusterInstanceRolePolicy 1185
Menggunakan kebijakan ini 1185
Rincian kebijakan 1185
Versi kebijakan 1186
Dokumen kebijakan JSON 1186
Pelajari selengkapnya 1188

AmazonSageMakerCoreServiceRolePolicy 1188
Menggunakan kebijakan ini 1188
Rincian kebijakan 1188
Versi kebijakan 1188
Dokumen kebijakan JSON 1189
Pelajari selengkapnya 1190
AmazonSageMakerEdgeDeviceFleetPolicy 1190
Menggunakan kebijakan ini 1190
Rincian kebijakan 1190
Versi kebijakan 1190
Dokumen kebijakan JSON 1190
Pelajari selengkapnya 1192
AmazonSageMakerFeatureStoreAccess 1192
Menggunakan kebijakan ini 1193
Rincian kebijakan 1193
Versi kebijakan 1193
Dokumen kebijakan JSON 1193
Pelajari selengkapnya 1194
AmazonSageMakerFullAccess 1194
Menggunakan kebijakan ini 1195
Rincian kebijakan 1195
Versi kebijakan 1195
Dokumen kebijakan JSON 1195
Pelajari selengkapnya 1211
AmazonSageMakerGeospatialExecutionRole 1212
Menggunakan kebijakan ini 1212
Rincian kebijakan 1212
Versi kebijakan 1212
Dokumen kebijakan JSON 1212
Pelajari selengkapnya 1213
AmazonSageMakerGeospatialFullAccess 1213
Menggunakan kebijakan ini 1213
Rincian kebijakan 1214
Versi kebijakan 1214
Dokumen kebijakan JSON 1214
Pelajari selengkapnya 1215

AmazonSageMakerGroundTruthExecution 1215
Menggunakan kebijakan ini 1215
Rincian kebijakan 1215
Versi kebijakan 1215
Dokumen kebijakan JSON 1216
Pelajari selengkapnya 1219
AmazonSageMakerHyperPodObservabilityAdminAccess 1219
Menggunakan kebijakan ini 1219
Rincian kebijakan 1220
Versi kebijakan 1220
Dokumen kebijakan JSON 1220
Pelajari selengkapnya 1226
AmazonSageMakerHyperPodServiceRolePolicy 1226
Menggunakan kebijakan ini 1226
Rincian kebijakan 1227
Versi kebijakan 1227
Dokumen kebijakan JSON 1227
Pelajari selengkapnya 1228
AmazonSageMakerMechanicalTurkAccess 1228
Menggunakan kebijakan ini 1228
Rincian kebijakan 1229
Versi kebijakan 1229
Dokumen kebijakan JSON 1229
Pelajari selengkapnya 1229
AmazonSageMakerModelGovernanceUseAccess 1230
Menggunakan kebijakan ini 1230
Rincian kebijakan 1230
Versi kebijakan 1230
Dokumen kebijakan JSON 1230
Pelajari selengkapnya 1232
AmazonSageMakerModelRegistryFullAccess 1232
Menggunakan kebijakan ini 1233
Rincian kebijakan 1233
Versi kebijakan 1233
Dokumen kebijakan JSON 1233
Pelajari selengkapnya 1237

AmazonSageMakerNotebooksServiceRolePolicy 1237
Menggunakan kebijakan ini 1237
Rincian kebijakan 1237
Versi kebijakan 1237
Dokumen kebijakan JSON 1238
Pelajari selengkapnya 1242
AmazonSageMakerPartnerAppsFullAccess 1242
Menggunakan kebijakan ini 1242
Rincian kebijakan 1242
Versi kebijakan 1243
Dokumen kebijakan JSON 1243
Pelajari selengkapnya 1244
AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy 1244
Menggunakan kebijakan ini 1244
Rincian kebijakan 1244
Versi kebijakan 1244
Dokumen kebijakan JSON 1245
Pelajari selengkapnya 1245
AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy 1246
Menggunakan kebijakan ini 1246
Rincian kebijakan 1246
Versi kebijakan 1246
Dokumen kebijakan JSON 1246
Pelajari selengkapnya 1250
AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy 1250
Menggunakan kebijakan ini 1250
Rincian kebijakan 1250
Versi kebijakan 1251
Dokumen kebijakan JSON 1251
Pelajari selengkapnya 1251
AmazonSageMakerPipelinesIntegrations 1252
Menggunakan kebijakan ini 1252
Rincian kebijakan 1252
Versi kebijakan 1252
Dokumen kebijakan JSON 1252
Pelajari selengkapnya 1254

AmazonSageMakerQuickSightVPCPolicy 1254
Menggunakan kebijakan ini 1255
Rincian kebijakan 1255
Versi kebijakan 1255
Dokumen kebijakan JSON 1255
Pelajari selengkapnya 1257
AmazonSageMakerReadOnly 1257
Menggunakan kebijakan ini 1257
Rincian kebijakan 1257
Versi kebijakan 1257
Dokumen kebijakan JSON 1257
Pelajari selengkapnya 1259
AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy 1259
Menggunakan kebijakan ini 1259
Rincian kebijakan 1259
Versi kebijakan 1259
Dokumen kebijakan JSON 1260
Pelajari selengkapnya 1260
AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy 1261
Menggunakan kebijakan ini 1261
Rincian kebijakan 1261
Versi kebijakan 1261
Dokumen kebijakan JSON 1261
Pelajari selengkapnya 1268
AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy 1268
Menggunakan kebijakan ini 1269
Rincian kebijakan 1269
Versi kebijakan 1269
Dokumen kebijakan JSON 1269
Pelajari selengkapnya 1279
AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy 1279
Menggunakan kebijakan ini 1280
Rincian kebijakan 1280
Versi kebijakan 1280
Dokumen kebijakan JSON 1280
Pelajari selengkapnya 1283

AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy 1283
Menggunakan kebijakan ini 1283
Rincian kebijakan 1284
Versi kebijakan 1284
Dokumen kebijakan JSON 1284
Pelajari selengkapnya 1284
AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy 1285
Menggunakan kebijakan ini 1285
Rincian kebijakan 1285
Versi kebijakan 1285
Dokumen kebijakan JSON 1285
Pelajari selengkapnya 1286
AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy 1286
Menggunakan kebijakan ini 1286
Rincian kebijakan 1286
Versi kebijakan 1287
Dokumen kebijakan JSON 1287
Pelajari selengkapnya 1289
AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy 1289
Menggunakan kebijakan ini 1289
Rincian kebijakan 1289
Versi kebijakan 1290
Dokumen kebijakan JSON 1290
Pelajari selengkapnya 1300
AmazonSageMakerTrainingPlanCreateAccess 1300
Menggunakan kebijakan ini 1300
Rincian kebijakan 1300
Versi kebijakan 1301
Dokumen kebijakan JSON 1301
Pelajari selengkapnya 1302
AmazonSecurityLakeAdministrator 1302
Menggunakan kebijakan ini 1303
Rincian kebijakan 1303
Versi kebijakan 1303
Dokumen kebijakan JSON 1303
Pelajari selengkapnya 1314

AmazonSecurityLakeMetastoreManager 1314
Menggunakan kebijakan ini 1315
Rincian kebijakan 1315
Versi kebijakan 1315
Dokumen kebijakan JSON 1315
Pelajari selengkapnya 1317
AmazonSecurityLakePermissionsBoundary 1318
Menggunakan kebijakan ini 1318
Rincian kebijakan 1318
Versi kebijakan 1318
Dokumen kebijakan JSON 1318
Pelajari selengkapnya 1321
AmazonSESFullAccess 1322
Menggunakan kebijakan ini 1322
Rincian kebijakan 1322
Versi kebijakan 1322
Dokumen kebijakan JSON 1322
Pelajari selengkapnya 1323
AmazonSESReadOnlyAccess 1323
Menggunakan kebijakan ini 1323
Rincian kebijakan 1323
Versi kebijakan 1323
Dokumen kebijakan JSON 1323
Pelajari selengkapnya 1324
AmazonSESServiceRolePolicy 1324
Menggunakan kebijakan ini 1324
Rincian kebijakan 1324
Versi kebijakan 1325
Dokumen kebijakan JSON 1325
Pelajari selengkapnya 1325
AmazonSNSFullAccess 1326
Menggunakan kebijakan ini 1326
Rincian kebijakan 1326
Versi kebijakan 1326
Dokumen kebijakan JSON 1326
Pelajari selengkapnya 1327

AmazonSNSReadOnlyAccess 1327
Menggunakan kebijakan ini 1327
Rincian kebijakan 1328
Versi kebijakan 1328
Dokumen kebijakan JSON 1328
Pelajari selengkapnya 1329
AmazonSNSRole 1329
Menggunakan kebijakan ini 1329
Rincian kebijakan 1329
Versi kebijakan 1330
Dokumen kebijakan JSON 1330
Pelajari selengkapnya 1330
AmazonSQSFullAccess 1330
Menggunakan kebijakan ini 1331
Rincian kebijakan 1331
Versi kebijakan 1331
Dokumen kebijakan JSON 1331
Pelajari selengkapnya 1331
AmazonSQSReadOnlyAccess 1332
Menggunakan kebijakan ini 1332
Rincian kebijakan 1332
Versi kebijakan 1332
Dokumen kebijakan JSON 1332
Pelajari selengkapnya 1333
AmazonSSMAutomationApproverAccess 1333
Menggunakan kebijakan ini 1333
Rincian kebijakan 1333
Versi kebijakan 1334
Dokumen kebijakan JSON 1334
Pelajari selengkapnya 1334
AmazonSSMAutomationRole 1334
Menggunakan kebijakan ini 1335
Rincian kebijakan 1335
Versi kebijakan 1335
Dokumen kebijakan JSON 1335
Pelajari selengkapnya 1337

AmazonSSMDirectoryServiceAccess 1337
Menggunakan kebijakan ini 1337
Rincian kebijakan 1337
Versi kebijakan 1337
Dokumen kebijakan JSON 1337
Pelajari selengkapnya 1338
AmazonSSMFullAccess 1338
Menggunakan kebijakan ini 1338
Rincian kebijakan 1338
Versi kebijakan 1339
Dokumen kebijakan JSON 1339
Pelajari selengkapnya 1340
AmazonSSMMaintenanceWindowRole 1340
Menggunakan kebijakan ini 1340
Rincian kebijakan 1340
Versi kebijakan 1341
Dokumen kebijakan JSON 1341
Pelajari selengkapnya 1342
AmazonSSMManagedEC2InstanceDefaultPolicy 1342
Menggunakan kebijakan ini 1343
Rincian kebijakan 1343
Versi kebijakan 1343
Dokumen kebijakan JSON 1343
Pelajari selengkapnya 1344
AmazonSSMManagedInstanceCore 1345
Menggunakan kebijakan ini 1345
Rincian kebijakan 1345
Versi kebijakan 1345
Dokumen kebijakan JSON 1345
Pelajari selengkapnya 1346
AmazonSSMPatchAssociation 1347
Menggunakan kebijakan ini 1347
Rincian kebijakan 1347
Versi kebijakan 1347
Dokumen kebijakan JSON 1347
Pelajari selengkapnya 1348

AmazonSSMReadOnlyAccess 1348
Menggunakan kebijakan ini 1348
Rincian kebijakan 1348
Versi kebijakan 1349
Dokumen kebijakan JSON 1349
Pelajari selengkapnya 1349
AmazonSSMServiceRolePolicy 1349
Menggunakan kebijakan ini 1350
Rincian kebijakan 1350
Versi kebijakan 1350
Dokumen kebijakan JSON 1350
Pelajari selengkapnya 1355
AmazonSumerianFullAccess 1355
Menggunakan kebijakan ini 1356
Rincian kebijakan 1356
Versi kebijakan 1356
Dokumen kebijakan JSON 1356
Pelajari selengkapnya 1356
AmazonTextractFullAccess 1357
Menggunakan kebijakan ini 1357
Rincian kebijakan 1357
Versi kebijakan 1357
Dokumen kebijakan JSON 1357
Pelajari selengkapnya 1358
AmazonTextractServiceRole 1358
Menggunakan kebijakan ini 1358
Rincian kebijakan 1358
Versi kebijakan 1358
Dokumen kebijakan JSON 1359
Pelajari selengkapnya 1359
AmazonTimestreamConsoleFullAccess 1359
Menggunakan kebijakan ini 1359
Rincian kebijakan 1359
Versi kebijakan 1360
Dokumen kebijakan JSON 1360
Pelajari selengkapnya 1362

AmazonTimestreamFullAccess 1362
Menggunakan kebijakan ini 1362
Rincian kebijakan 1362
Versi kebijakan 1363
Dokumen kebijakan JSON 1363
Pelajari selengkapnya 1364
AmazonTimestreamInfluxDBFullAccess 1364
Menggunakan kebijakan ini 1364
Rincian kebijakan 1364
Versi kebijakan 1365
Dokumen kebijakan JSON 1365
Pelajari selengkapnya 1367
AmazonTimestreamInfluxDBFullAccessWithoutMarketplaceAccess 1368
Menggunakan kebijakan ini 1368
Rincian kebijakan 1368
Versi kebijakan 1368
Dokumen kebijakan JSON 1368
Pelajari selengkapnya 1370
AmazonTimestreamInfluxDBServiceRolePolicy 1371
Menggunakan kebijakan ini 1371
Rincian kebijakan 1371
Versi kebijakan 1371
Dokumen kebijakan JSON 1371
Pelajari selengkapnya 1374
AmazonTimestreamReadOnlyAccess 1374
Menggunakan kebijakan ini 1374
Rincian kebijakan 1374
Versi kebijakan 1375
Dokumen kebijakan JSON 1375
Pelajari selengkapnya 1375
AmazonTranscribeFullAccess 1376
Menggunakan kebijakan ini 1376
Rincian kebijakan 1376
Versi kebijakan 1376
Dokumen kebijakan JSON 1376
Pelajari selengkapnya 1377

AmazonTranscribeReadOnlyAccess 1377
Menggunakan kebijakan ini 1377
Rincian kebijakan 1377
Versi kebijakan 1378
Dokumen kebijakan JSON 1378
Pelajari selengkapnya 1378
AmazonVerifiedPermissionsFullAccess 1378
Menggunakan kebijakan ini 1379
Rincian kebijakan 1379
Versi kebijakan 1379
Dokumen kebijakan JSON 1379
Pelajari selengkapnya 1380
AmazonVerifiedPermissionsReadOnlyAccess 1380
Menggunakan kebijakan ini 1380
Rincian kebijakan 1380
Versi kebijakan 1380
Dokumen kebijakan JSON 1381
Pelajari selengkapnya 1381
AmazonVPCCrossAccountNetworkInterfaceOperations 1382
Menggunakan kebijakan ini 1382
Rincian kebijakan 1382
Versi kebijakan 1382
Dokumen kebijakan JSON 1382
Pelajari selengkapnya 1384
AmazonVPCFullAccess 1384
Menggunakan kebijakan ini 1384
Rincian kebijakan 1384
Versi kebijakan 1384
Dokumen kebijakan JSON 1385
Pelajari selengkapnya 1389
AmazonVPCNetworkAccessAnalyzerFullAccessPolicy 1389
Menggunakan kebijakan ini 1389
Rincian kebijakan 1389
Versi kebijakan 1389
Dokumen kebijakan JSON 1390
Pelajari selengkapnya 1393

AmazonVPCReachabilityAnalyzerFullAccessPolicy 1393
Menggunakan kebijakan ini 1393
Rincian kebijakan 1393
Versi kebijakan 1394
Dokumen kebijakan JSON 1394
Pelajari selengkapnya 1397
AmazonVPCReachabilityAnalyzerPathComponentReadPolicy 1397
Menggunakan kebijakan ini 1397
Rincian kebijakan 1397
Versi kebijakan 1398
Dokumen kebijakan JSON 1398
Pelajari selengkapnya 1398
AmazonVPCReadOnlyAccess 1398
Menggunakan kebijakan ini 1399
Rincian kebijakan 1399
Versi kebijakan 1399
Dokumen kebijakan JSON 1399
Pelajari selengkapnya 1400
AmazonWorkDocsFullAccess 1401
Menggunakan kebijakan ini 1401
Rincian kebijakan 1401
Versi kebijakan 1401
Dokumen kebijakan JSON 1401
Pelajari selengkapnya 1402
AmazonWorkDocsReadOnlyAccess 1402
Menggunakan kebijakan ini 1402
Rincian kebijakan 1402
Versi kebijakan 1402
Dokumen kebijakan JSON 1403
Pelajari selengkapnya 1403
AmazonWorkMailEventsServiceRolePolicy 1403
Menggunakan kebijakan ini 1403
Rincian kebijakan 1404
Versi kebijakan 1404
Dokumen kebijakan JSON 1404
Pelajari selengkapnya 1404

AmazonWorkMailFullAccess 1405
Menggunakan kebijakan ini 1405
Rincian kebijakan 1405
Versi kebijakan 1405
Dokumen kebijakan JSON 1405
Pelajari selengkapnya 1407
AmazonWorkMailMessageFlowFullAccess 1407
Menggunakan kebijakan ini 1408
Rincian kebijakan 1408
Versi kebijakan 1408
Dokumen kebijakan JSON 1408
Pelajari selengkapnya 1408
AmazonWorkMailMessageFlowReadOnlyAccess 1409
Menggunakan kebijakan ini 1409
Rincian kebijakan 1409
Versi kebijakan 1409
Dokumen kebijakan JSON 1409
Pelajari selengkapnya 1410
AmazonWorkMailReadOnlyAccess 1410
Menggunakan kebijakan ini 1410
Rincian kebijakan 1410
Versi kebijakan 1410
Dokumen kebijakan JSON 1411
Pelajari selengkapnya 1411
AmazonWorkSpacesAdmin 1411
Menggunakan kebijakan ini 1412
Rincian kebijakan 1412
Versi kebijakan 1412
Dokumen kebijakan JSON 1412
Pelajari selengkapnya 1413
AmazonWorkSpacesApplicationManagerAdminAccess 1414
Menggunakan kebijakan ini 1414
Rincian kebijakan 1414
Versi kebijakan 1414
Dokumen kebijakan JSON 1414
Pelajari selengkapnya 1415

AmazonWorkspacesPCAAccess 1415
Menggunakan kebijakan ini 1415
Rincian kebijakan 1415
Versi kebijakan 1415
Dokumen kebijakan JSON 1416
Pelajari selengkapnya 1416
AmazonWorkSpacesPoolServiceAccess 1416
Menggunakan kebijakan ini 1417
Rincian kebijakan 1417
Versi kebijakan 1417
Dokumen kebijakan JSON 1417
Pelajari selengkapnya 1418
AmazonWorkSpacesSecureBrowserReadOnly 1419
Menggunakan kebijakan ini 1419
Rincian kebijakan 1419
Versi kebijakan 1419
Dokumen kebijakan JSON 1419
Pelajari selengkapnya 1420
AmazonWorkSpacesSelfServiceAccess 1421
Menggunakan kebijakan ini 1421
Rincian kebijakan 1421
Versi kebijakan 1421
Dokumen kebijakan JSON 1421
Pelajari selengkapnya 1422
AmazonWorkSpacesServiceAccess 1422
Menggunakan kebijakan ini 1422
Rincian kebijakan 1422
Versi kebijakan 1422
Dokumen kebijakan JSON 1423
Pelajari selengkapnya 1423
AmazonWorkSpacesThinClientFullAccess 1423
Menggunakan kebijakan ini 1423
Rincian kebijakan 1423
Versi kebijakan 1424
Dokumen kebijakan JSON 1424
Pelajari selengkapnya 1425

AmazonWorkSpacesThinClientMonitoringServiceRolePolicy 1425
Menggunakan kebijakan ini 1425
Rincian kebijakan 1425
Versi kebijakan 1426
Dokumen kebijakan JSON 1426
Pelajari selengkapnya 1426
AmazonWorkSpacesThinClientReadOnlyAccess 1427
Menggunakan kebijakan ini 1427
Rincian kebijakan 1427
Versi kebijakan 1427
Dokumen kebijakan JSON 1427
Pelajari selengkapnya 1428
AmazonWorkSpacesWebReadOnly 1429
Menggunakan kebijakan ini 1429
Rincian kebijakan 1429
Versi kebijakan 1429
Dokumen kebijakan JSON 1429
Pelajari selengkapnya 1430
AmazonWorkSpacesWebServiceRolePolicy 1431
Menggunakan kebijakan ini 1431
Rincian kebijakan 1431
Versi kebijakan 1431
Dokumen kebijakan JSON 1431
Pelajari selengkapnya 1434
AmazonZocaloFullAccess 1434
Menggunakan kebijakan ini 1434
Rincian kebijakan 1434
Versi kebijakan 1434
Dokumen kebijakan JSON 1434
Pelajari selengkapnya 1435
AmazonZocaloReadOnlyAccess 1435
Menggunakan kebijakan ini 1435
Rincian kebijakan 1436
Versi kebijakan 1436
Dokumen kebijakan JSON 1436
Pelajari selengkapnya 1436

AmplifyBackendDeployFullAccess 1437
Menggunakan kebijakan ini 1437
Rincian kebijakan 1437
Versi kebijakan 1437
Dokumen kebijakan JSON 1437
Pelajari selengkapnya 1442
APIGatewayServiceRolePolicy 1442
Menggunakan kebijakan ini 1442
Rincian kebijakan 1442
Versi kebijakan 1442
Dokumen kebijakan JSON 1443
Pelajari selengkapnya 1445
AppIntegrationsServiceLinkedRolePolicy 1445
Menggunakan kebijakan ini 1445
Rincian kebijakan 1445
Versi kebijakan 1445
Dokumen kebijakan JSON 1446
Pelajari selengkapnya 1447
ApplicationAutoScalingForAmazonAppStreamAccess 1447
Menggunakan kebijakan ini 1448
Rincian kebijakan 1448
Versi kebijakan 1448
Dokumen kebijakan JSON 1448
Pelajari selengkapnya 1449
ApplicationDiscoveryServiceContinuousExportServiceRolePolicy 1449
Menggunakan kebijakan ini 1449
Rincian kebijakan 1449
Versi kebijakan 1450
Dokumen kebijakan JSON 1450
Pelajari selengkapnya 1452
AppRunnerNetworkingServiceRolePolicy 1452
Menggunakan kebijakan ini 1452
Rincian kebijakan 1452
Versi kebijakan 1452
Dokumen kebijakan JSON 1453
Pelajari selengkapnya 1454

AppRunnerServiceRolePolicy 1454
Menggunakan kebijakan ini 1454
Rincian kebijakan 1454
Versi kebijakan 1455
Dokumen kebijakan JSON 1455
Pelajari selengkapnya 1456
AppStudioServiceRolePolicy 1456
Menggunakan kebijakan ini 1456
Rincian kebijakan 1456
Versi kebijakan 1456
Dokumen kebijakan JSON 1457
Pelajari selengkapnya 1459
AuroraDsqlServiceLinkedRolePolicy 1459
Menggunakan kebijakan ini 1459
Rincian kebijakan 1459
Versi kebijakan 1459
Dokumen kebijakan JSON 1460
Pelajari selengkapnya 1460
AutoScalingConsoleFullAccess 1460
Menggunakan kebijakan ini 1461
Rincian kebijakan 1461
Versi kebijakan 1461
Dokumen kebijakan JSON 1461
Pelajari selengkapnya 1463
AutoScalingConsoleReadOnlyAccess 1463
Menggunakan kebijakan ini 1463
Rincian kebijakan 1463
Versi kebijakan 1463
Dokumen kebijakan JSON 1464
Pelajari selengkapnya 1465
AutoScalingFullAccess 1465
Menggunakan kebijakan ini 1465
Rincian kebijakan 1465
Versi kebijakan 1465
Dokumen kebijakan JSON 1466
Pelajari selengkapnya 1467

AutoScalingNotificationAccessRole 1467
Menggunakan kebijakan ini 1467
Rincian kebijakan 1467
Versi kebijakan 1468
Dokumen kebijakan JSON 1468
Pelajari selengkapnya 1468
AutoScalingReadOnlyAccess 1468
Menggunakan kebijakan ini 1469
Rincian kebijakan 1469
Versi kebijakan 1469
Dokumen kebijakan JSON 1469
Pelajari selengkapnya 1469
AutoScalingServiceRolePolicy 1470
Menggunakan kebijakan ini 1470
Rincian kebijakan 1470
Versi kebijakan 1470
Dokumen kebijakan JSON 1470
Pelajari selengkapnya 1473
AWS-SSM-Automation-DiagnosisBucketPolicy 1473
Menggunakan kebijakan ini 1474
Rincian kebijakan 1474
Versi kebijakan 1474
Dokumen kebijakan JSON 1474
Pelajari selengkapnya 1476
AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy 1477
Menggunakan kebijakan ini 1477
Rincian kebijakan 1477
Versi kebijakan 1477
Dokumen kebijakan JSON 1477
Pelajari selengkapnya 1480
AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy 1480
Menggunakan kebijakan ini 1480
Rincian kebijakan 1480
Versi kebijakan 1481
Dokumen kebijakan JSON 1481
Pelajari selengkapnya 1483

AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrationRolePolicy 1483
Menggunakan kebijakan ini 1483
Rincian kebijakan 1483
Versi kebijakan 1483
Dokumen kebijakan JSON 1484
Pelajari selengkapnya 1484
AWS-SSM-RemediationAutomation-AdministrationRolePolicy 1485
Menggunakan kebijakan ini 1485
Rincian kebijakan 1485
Versi kebijakan 1485
Dokumen kebijakan JSON 1485
Pelajari selengkapnya 1488
AWS-SSM-RemediationAutomation-ExecutionRolePolicy 1488
Menggunakan kebijakan ini 1488
Rincian kebijakan 1488
Versi kebijakan 1489
Dokumen kebijakan JSON 1489
Pelajari selengkapnya 1495
AWS-SSM-RemediationAutomation-OperationalAccountAdministrationRolePolicy 1495
Menggunakan kebijakan ini 1495
Rincian kebijakan 1495
Versi kebijakan 1496
Dokumen kebijakan JSON 1496
Pelajari selengkapnya 1497
AWS_ConfigRole 1497
Menggunakan kebijakan ini 1497
Rincian kebijakan 1497
Versi kebijakan 1497
Dokumen kebijakan JSON 1497
Pelajari selengkapnya 1534
AWSAccountActivityAccess 1535
Menggunakan kebijakan ini 1535
Rincian kebijakan 1535
Versi kebijakan 1535
Dokumen kebijakan JSON 1535
Pelajari selengkapnya 1536

AWSAccountManagementFullAccess 1536
Menggunakan kebijakan ini 1536
Rincian kebijakan 1536
Versi kebijakan 1537
Dokumen kebijakan JSON 1537
Pelajari selengkapnya 1537
AWSAccountManagementReadOnlyAccess 1537
Menggunakan kebijakan ini 1537
Rincian kebijakan 1538
Versi kebijakan 1538
Dokumen kebijakan JSON 1538
Pelajari selengkapnya 1538
AWSAccountUsageReportAccess 1539
Menggunakan kebijakan ini 1539
Rincian kebijakan 1539
Versi kebijakan 1539
Dokumen kebijakan JSON 1539
Pelajari selengkapnya 1540
AWSAgentlessDiscoveryService 1540
Menggunakan kebijakan ini 1540
Rincian kebijakan 1540
Versi kebijakan 1540
Dokumen kebijakan JSON 1540
Pelajari selengkapnya 1542
AWSAppFabricFullAccess 1543
Menggunakan kebijakan ini 1543
Rincian kebijakan 1543
Versi kebijakan 1543
Dokumen kebijakan JSON 1543
Pelajari selengkapnya 1545
AWSAppFabricReadOnlyAccess 1545
Menggunakan kebijakan ini 1545
Rincian kebijakan 1545
Versi kebijakan 1545
Dokumen kebijakan JSON 1545
Pelajari selengkapnya 1546

AWSAppFabricServiceRolePolicy 1546
Menggunakan kebijakan ini 1546
Rincian kebijakan 1546
Versi kebijakan 1547
Dokumen kebijakan JSON 1547
Pelajari selengkapnya 1548
AWSApplicationAutoscalingAppStreamFleetPolicy 1548
Menggunakan kebijakan ini 1548
Rincian kebijakan 1548
Versi kebijakan 1549
Dokumen kebijakan JSON 1549
Pelajari selengkapnya 1549
AWSApplicationAutoscalingCassandraTablePolicy 1550
Menggunakan kebijakan ini 1550
Rincian kebijakan 1550
Versi kebijakan 1550
Dokumen kebijakan JSON 1550
Pelajari selengkapnya 1551
AWSApplicationAutoscalingComprehendEndpointPolicy 1551
Menggunakan kebijakan ini 1551
Rincian kebijakan 1551
Versi kebijakan 1552
Dokumen kebijakan JSON 1552
Pelajari selengkapnya 1552
AWSApplicationAutoScalingCustomResourcePolicy 1553
Menggunakan kebijakan ini 1553
Rincian kebijakan 1553
Versi kebijakan 1553
Dokumen kebijakan JSON 1553
Pelajari selengkapnya 1554
AWSApplicationAutoscalingDynamoDBTablePolicy 1554
Menggunakan kebijakan ini 1554
Rincian kebijakan 1554
Versi kebijakan 1555
Dokumen kebijakan JSON 1555
Pelajari selengkapnya 1555

AWSApplicationAutoscalingEC2SpotFleetRequestPolicy 1555
Menggunakan kebijakan ini 1556
Rincian kebijakan 1556
Versi kebijakan 1556
Dokumen kebijakan JSON 1556
Pelajari selengkapnya 1557
AWSApplicationAutoscalingECSServicePolicy 1557
Menggunakan kebijakan ini 1557
Rincian kebijakan 1557
Versi kebijakan 1557
Dokumen kebijakan JSON 1558
Pelajari selengkapnya 1558
AWSApplicationAutoscalingElastiCacheRGPolicy 1558
Menggunakan kebijakan ini 1558
Rincian kebijakan 1559
Versi kebijakan 1559
Dokumen kebijakan JSON 1559
Pelajari selengkapnya 1560
AWSApplicationAutoscalingEMRInstanceGroupPolicy 1560
Menggunakan kebijakan ini 1560
Rincian kebijakan 1561
Versi kebijakan 1561
Dokumen kebijakan JSON 1561
Pelajari selengkapnya 1561
AWSApplicationAutoscalingKafkaClusterPolicy 1562
Menggunakan kebijakan ini 1562
Rincian kebijakan 1562
Versi kebijakan 1562
Dokumen kebijakan JSON 1562
Pelajari selengkapnya 1563
AWSApplicationAutoscalingLambdaConcurrencyPolicy 1563
Menggunakan kebijakan ini 1563
Rincian kebijakan 1563
Versi kebijakan 1564
Dokumen kebijakan JSON 1564
Pelajari selengkapnya 1564

AWSApplicationAutoscalingNeptuneClusterPolicy 1564
Menggunakan kebijakan ini 1565
Rincian kebijakan 1565
Versi kebijakan 1565
Dokumen kebijakan JSON 1565
Pelajari selengkapnya 1567
AWSApplicationAutoscalingRDSClusterPolicy 1567
Menggunakan kebijakan ini 1567
Rincian kebijakan 1567
Versi kebijakan 1567
Dokumen kebijakan JSON 1568
Pelajari selengkapnya 1568
AWSApplicationAutoscalingSageMakerEndpointPolicy 1569
Menggunakan kebijakan ini 1569
Rincian kebijakan 1569
Versi kebijakan 1569
Dokumen kebijakan JSON 1569
Pelajari selengkapnya 1570
AWSApplicationAutoscalingWorkSpacesPoolPolicy 1570
Menggunakan kebijakan ini 1571
Rincian kebijakan 1571
Versi kebijakan 1571
Dokumen kebijakan JSON 1571
Pelajari selengkapnya 1572
AWSApplicationDiscoveryAgentAccess 1573
Menggunakan kebijakan ini 1573
Rincian kebijakan 1573
Versi kebijakan 1573
Dokumen kebijakan JSON 1573
Pelajari selengkapnya 1574
AWSApplicationDiscoveryAgentlessCollectorAccess 1574
Menggunakan kebijakan ini 1574
Rincian kebijakan 1574
Versi kebijakan 1575
Dokumen kebijakan JSON 1575
Pelajari selengkapnya 1576

AWSApplicationDiscoveryServiceFullAccess 1576
Menggunakan kebijakan ini 1576
Rincian kebijakan 1576
Versi kebijakan 1576
Dokumen kebijakan JSON 1577
Pelajari selengkapnya 1578
AWSApplicationMigrationAgentInstallationPolicy 1578
Menggunakan kebijakan ini 1579
Rincian kebijakan 1579
Versi kebijakan 1579
Dokumen kebijakan JSON 1579
Pelajari selengkapnya 1580
AWSApplicationMigrationAgentPolicy 1580
Menggunakan kebijakan ini 1580
Rincian kebijakan 1581
Versi kebijakan 1581
Dokumen kebijakan JSON 1581
Pelajari selengkapnya 1582
AWSApplicationMigrationAgentPolicy_v2 1582
Menggunakan kebijakan ini 1582
Rincian kebijakan 1582
Versi kebijakan 1583
Dokumen kebijakan JSON 1583
Pelajari selengkapnya 1583
AWSApplicationMigrationConversionServerPolicy 1584
Menggunakan kebijakan ini 1584
Rincian kebijakan 1584
Versi kebijakan 1584
Dokumen kebijakan JSON 1585
Pelajari selengkapnya 1585
AWSApplicationMigrationEC2Access 1585
Menggunakan kebijakan ini 1585
Rincian kebijakan 1586
Versi kebijakan 1586
Dokumen kebijakan JSON 1586
Pelajari selengkapnya 1594

AWSApplicationMigrationFullAccess 1594
Menggunakan kebijakan ini 1594
Rincian kebijakan 1595
Versi kebijakan 1595
Dokumen kebijakan JSON 1595
Pelajari selengkapnya 1601
AWSApplicationMigrationMGHAccess 1601
Menggunakan kebijakan ini 1601
Rincian kebijakan 1602
Versi kebijakan 1602
Dokumen kebijakan JSON 1602
Pelajari selengkapnya 1603
AWSApplicationMigrationReadOnlyAccess 1603
Menggunakan kebijakan ini 1603
Rincian kebijakan 1603
Versi kebijakan 1603
Dokumen kebijakan JSON 1604
Pelajari selengkapnya 1605
AWSApplicationMigrationReplicationServerPolicy 1605
Menggunakan kebijakan ini 1605
Rincian kebijakan 1605
Versi kebijakan 1606
Dokumen kebijakan JSON 1606
Pelajari selengkapnya 1607
AWSApplicationMigrationServiceEc2InstancePolicy 1608
Menggunakan kebijakan ini 1608
Rincian kebijakan 1608
Versi kebijakan 1608
Dokumen kebijakan JSON 1608
Pelajari selengkapnya 1609
AWSApplicationMigrationServiceRolePolicy 1610
Menggunakan kebijakan ini 1610
Rincian kebijakan 1610
Versi kebijakan 1610
Dokumen kebijakan JSON 1610
Pelajari selengkapnya 1618

AWSApplicationMigrationSSMAccess 1618
Menggunakan kebijakan ini 1618
Rincian kebijakan 1618
Versi kebijakan 1618
Dokumen kebijakan JSON 1619
Pelajari selengkapnya 1620
AWSApplicationMigrationVCenterClientPolicy 1621
Menggunakan kebijakan ini 1621
Rincian kebijakan 1621
Versi kebijakan 1621
Dokumen kebijakan JSON 1621
Pelajari selengkapnya 1622
AWSAppMeshEnvoyAccess 1622
Menggunakan kebijakan ini 1622
Rincian kebijakan 1623
Versi kebijakan 1623
Dokumen kebijakan JSON 1623
Pelajari selengkapnya 1623
AWSAppMeshFullAccess 1624
Menggunakan kebijakan ini 1624
Rincian kebijakan 1624
Versi kebijakan 1624
Dokumen kebijakan JSON 1624
Pelajari selengkapnya 1626
AWSAppMeshPreviewEnvoyAccess 1626
Menggunakan kebijakan ini 1626
Rincian kebijakan 1626
Versi kebijakan 1626
Dokumen kebijakan JSON 1626
Pelajari selengkapnya 1627
AWSAppMeshPreviewServiceRolePolicy 1627
Menggunakan kebijakan ini 1627
Rincian kebijakan 1627
Versi kebijakan 1628
Dokumen kebijakan JSON 1628
Pelajari selengkapnya 1628

AWSAppMeshReadOnly 1628
Menggunakan kebijakan ini 1629
Rincian kebijakan 1629
Versi kebijakan 1629
Dokumen kebijakan JSON 1629
Pelajari selengkapnya 1630
AWSAppMeshServiceRolePolicy 1630
Menggunakan kebijakan ini 1631
Rincian kebijakan 1631
Versi kebijakan 1631
Dokumen kebijakan JSON 1631
Pelajari selengkapnya 1632
AWSAppRunnerFullAccess 1632
Menggunakan kebijakan ini 1632
Rincian kebijakan 1632
Versi kebijakan 1632
Dokumen kebijakan JSON 1633
Pelajari selengkapnya 1633
AWSAppRunnerReadOnlyAccess 1634
Menggunakan kebijakan ini 1634
Rincian kebijakan 1634
Versi kebijakan 1634
Dokumen kebijakan JSON 1634
Pelajari selengkapnya 1635
AWSAppRunnerServicePolicyForECRAccess 1635
Menggunakan kebijakan ini 1635
Rincian kebijakan 1635
Versi kebijakan 1635
Dokumen kebijakan JSON 1636
Pelajari selengkapnya 1636
AWSAppSyncAdministrator 1636
Menggunakan kebijakan ini 1636
Rincian kebijakan 1637
Versi kebijakan 1637
Dokumen kebijakan JSON 1637
Pelajari selengkapnya 1638

AWSAppSyncInvokeFullAccess 1638
Menggunakan kebijakan ini 1638
Rincian kebijakan 1639
Versi kebijakan 1639
Dokumen kebijakan JSON 1639
Pelajari selengkapnya 1639
AWSAppSyncPushToCloudWatchLogs 1640
Menggunakan kebijakan ini 1640
Rincian kebijakan 1640
Versi kebijakan 1640
Dokumen kebijakan JSON 1640
Pelajari selengkapnya 1641
AWSAppSyncSchemaAuthor 1641
Menggunakan kebijakan ini 1641
Rincian kebijakan 1641
Versi kebijakan 1641
Dokumen kebijakan JSON 1642
Pelajari selengkapnya 1643
AWSAppSyncServiceRolePolicy 1643
Menggunakan kebijakan ini 1643
Rincian kebijakan 1643
Versi kebijakan 1643
Dokumen kebijakan JSON 1644
Pelajari selengkapnya 1644
AWSArtifactAccountSync 1644
Menggunakan kebijakan ini 1644
Rincian kebijakan 1644
Versi kebijakan 1645
Dokumen kebijakan JSON 1645
Pelajari selengkapnya 1645
AWSArtifactAgreementsFullAccess 1645
Menggunakan kebijakan ini 1646
Rincian kebijakan 1646
Versi kebijakan 1646
Dokumen kebijakan JSON 1646
Pelajari selengkapnya 1648

AWSArtifactAgreementsReadOnlyAccess 1648
Menggunakan kebijakan ini 1648
Rincian kebijakan 1648
Versi kebijakan 1649
Dokumen kebijakan JSON 1649
Pelajari selengkapnya 1650
AWSArtifactReportsReadOnlyAccess 1650
Menggunakan kebijakan ini 1650
Rincian kebijakan 1650
Versi kebijakan 1651
Dokumen kebijakan JSON 1651
Pelajari selengkapnya 1651
AWSArtifactServiceRolePolicy 1651
Menggunakan kebijakan ini 1652
Rincian kebijakan 1652
Versi kebijakan 1652
Dokumen kebijakan JSON 1652
Pelajari selengkapnya 1653
AWSAuditManagerAdministratorAccess 1653
Menggunakan kebijakan ini 1653
Rincian kebijakan 1653
Versi kebijakan 1653
Dokumen kebijakan JSON 1653
Pelajari selengkapnya 1657
AWSAuditManagerServiceRolePolicy 1658
Menggunakan kebijakan ini 1658
Rincian kebijakan 1658
Versi kebijakan 1658
Dokumen kebijakan JSON 1658
Pelajari selengkapnya 1665
AWSAutoScalingPlansEC2AutoScalingPolicy 1665
Menggunakan kebijakan ini 1665
Rincian kebijakan 1666
Versi kebijakan 1666
Dokumen kebijakan JSON 1666
Pelajari selengkapnya 1666

AWSBackupAuditAccess 1667
Menggunakan kebijakan ini 1667
Rincian kebijakan 1667
Versi kebijakan 1667
Dokumen kebijakan JSON 1667
Pelajari selengkapnya 1669
AWSBackupDataTransferAccess 1669
Menggunakan kebijakan ini 1669
Rincian kebijakan 1669
Versi kebijakan 1669
Dokumen kebijakan JSON 1670
Pelajari selengkapnya 1670
AWSBackupFullAccess 1670
Menggunakan kebijakan ini 1670
Rincian kebijakan 1671
Versi kebijakan 1671
Dokumen kebijakan JSON 1671
Pelajari selengkapnya 1682
AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync 1682
Menggunakan kebijakan ini 1683
Rincian kebijakan 1683
Versi kebijakan 1683
Dokumen kebijakan JSON 1683
Pelajari selengkapnya 1684
AWSBackupOperatorAccess 1684
Menggunakan kebijakan ini 1684
Rincian kebijakan 1684
Versi kebijakan 1684
Dokumen kebijakan JSON 1685
Pelajari selengkapnya 1693
AWSBackupOrganizationAdminAccess 1693
Menggunakan kebijakan ini 1694
Rincian kebijakan 1694
Versi kebijakan 1694
Dokumen kebijakan JSON 1694
Pelajari selengkapnya 1696

AWSBackupRestoreAccessForSAPHANA 1696
Menggunakan kebijakan ini 1696
Rincian kebijakan 1696
Versi kebijakan 1697
Dokumen kebijakan JSON 1697
Pelajari selengkapnya 1698
AWSBackupSearchOperatorAccess 1698
Menggunakan kebijakan ini 1698
Rincian kebijakan 1698
Versi kebijakan 1698
Dokumen kebijakan JSON 1699
Pelajari selengkapnya 1700
AWSBackupServiceLinkedRolePolicyForBackup 1700
Menggunakan kebijakan ini 1701
Rincian kebijakan 1701
Versi kebijakan 1701
Dokumen kebijakan JSON 1701
Pelajari selengkapnya 1710
AWSBackupServiceLinkedRolePolicyForBackupTest 1711
Menggunakan kebijakan ini 1711
Rincian kebijakan 1711
Versi kebijakan 1711
Dokumen kebijakan JSON 1711
Pelajari selengkapnya 1712
AWSBackupServiceRolePolicyForBackup 1712
Menggunakan kebijakan ini 1712
Rincian kebijakan 1712
Versi kebijakan 1713
Dokumen kebijakan JSON 1713
Pelajari selengkapnya 1726
AWSBackupServiceRolePolicyForIndexing 1726
Menggunakan kebijakan ini 1727
Rincian kebijakan 1727
Versi kebijakan 1727
Dokumen kebijakan JSON 1727
Pelajari selengkapnya 1728

AWSBackupServiceRolePolicyForItemRestores 1728
Menggunakan kebijakan ini 1729
Rincian kebijakan 1729
Versi kebijakan 1729
Dokumen kebijakan JSON 1729
Pelajari selengkapnya 1731
AWSBackupServiceRolePolicyForRestores 1731
Menggunakan kebijakan ini 1731
Rincian kebijakan 1731
Versi kebijakan 1732
Dokumen kebijakan JSON 1732
Pelajari selengkapnya 1743
AWSBackupServiceRolePolicyForS3Backup 1743
Menggunakan kebijakan ini 1744
Rincian kebijakan 1744
Versi kebijakan 1744
Dokumen kebijakan JSON 1744
Pelajari selengkapnya 1746
AWSBackupServiceRolePolicyForS3Restore 1747
Menggunakan kebijakan ini 1747
Rincian kebijakan 1747
Versi kebijakan 1747
Dokumen kebijakan JSON 1747
Pelajari selengkapnya 1749
AWSBatchFullAccess 1749
Menggunakan kebijakan ini 1749
Rincian kebijakan 1749
Versi kebijakan 1749
Dokumen kebijakan JSON 1749
Pelajari selengkapnya 1751
AWSBatchServiceEventTargetRole 1751
Menggunakan kebijakan ini 1751
Rincian kebijakan 1751
Versi kebijakan 1752
Dokumen kebijakan JSON 1752
Pelajari selengkapnya 1752

AWSBatchServiceRole 1752
Menggunakan kebijakan ini 1753
Rincian kebijakan 1753
Versi kebijakan 1753
Dokumen kebijakan JSON 1753
Pelajari selengkapnya 1756
AWSBCMDataExportsServiceRolePolicy 1756
Menggunakan kebijakan ini 1757
Rincian kebijakan 1757
Versi kebijakan 1757
Dokumen kebijakan JSON 1757
Pelajari selengkapnya 1758
AWSBillingConductorFullAccess 1758
Menggunakan kebijakan ini 1758
Rincian kebijakan 1758
Versi kebijakan 1758
Dokumen kebijakan JSON 1758
Pelajari selengkapnya 1759
AWSBillingConductorReadOnlyAccess 1759
Menggunakan kebijakan ini 1759
Rincian kebijakan 1759
Versi kebijakan 1760
Dokumen kebijakan JSON 1760
Pelajari selengkapnya 1760
AWSBillingReadOnlyAccess 1760
Menggunakan kebijakan ini 1761
Rincian kebijakan 1761
Versi kebijakan 1761
Dokumen kebijakan JSON 1761
Pelajari selengkapnya 1763
AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM 1763
Menggunakan kebijakan ini 1763
Rincian kebijakan 1764
Versi kebijakan 1764
Dokumen kebijakan JSON 1764
Pelajari selengkapnya 1765

AWSBudgetsActionsWithAWSResourceControlAccess 1765
Menggunakan kebijakan ini 1765
Rincian kebijakan 1765
Versi kebijakan 1766
Dokumen kebijakan JSON 1766
Pelajari selengkapnya 1767
AWSBudgetsReadOnlyAccess 1767
Menggunakan kebijakan ini 1767
Rincian kebijakan 1768
Versi kebijakan 1768
Dokumen kebijakan JSON 1768
Pelajari selengkapnya 1768
AWSBugBustFullAccess 1769
Menggunakan kebijakan ini 1769
Rincian kebijakan 1769
Versi kebijakan 1769
Dokumen kebijakan JSON 1769
Pelajari selengkapnya 1770
AWSBugBustPlayerAccess 1771
Menggunakan kebijakan ini 1771
Rincian kebijakan 1771
Versi kebijakan 1771
Dokumen kebijakan JSON 1771
Pelajari selengkapnya 1772
AWSBugBustServiceRolePolicy 1772
Menggunakan kebijakan ini 1773
Rincian kebijakan 1773
Versi kebijakan 1773
Dokumen kebijakan JSON 1773
Pelajari selengkapnya 1774
AWSCertificateManagerFullAccess 1774
Menggunakan kebijakan ini 1774
Rincian kebijakan 1774
Versi kebijakan 1774
Dokumen kebijakan JSON 1775
Pelajari selengkapnya 1775

AWSCertificateManagerPrivateCAAuditor 1776
Menggunakan kebijakan ini 1776
Rincian kebijakan 1776
Versi kebijakan 1776
Dokumen kebijakan JSON 1776
Pelajari selengkapnya 1777
AWSCertificateManagerPrivateCAFullAccess 1777
Menggunakan kebijakan ini 1777
Rincian kebijakan 1777
Versi kebijakan 1778
Dokumen kebijakan JSON 1778
Pelajari selengkapnya 1778
AWSCertificateManagerPrivateCAPrivilegedUser 1778
Menggunakan kebijakan ini 1779
Rincian kebijakan 1779
Versi kebijakan 1779
Dokumen kebijakan JSON 1779
Pelajari selengkapnya 1780
AWSCertificateManagerPrivateCAReadOnly 1781
Menggunakan kebijakan ini 1781
Rincian kebijakan 1781
Versi kebijakan 1781
Dokumen kebijakan JSON 1781
Pelajari selengkapnya 1782
AWSCertificateManagerPrivateCAUser 1782
Menggunakan kebijakan ini 1782
Rincian kebijakan 1782
Versi kebijakan 1782
Dokumen kebijakan JSON 1783
Pelajari selengkapnya 1784
AWSCertificateManagerReadOnly 1784
Menggunakan kebijakan ini 1784
Rincian kebijakan 1784
Versi kebijakan 1785
Dokumen kebijakan JSON 1785
Pelajari selengkapnya 1785

AWSChatbotServiceLinkedRolePolicy 1785
Menggunakan kebijakan ini 1786
Rincian kebijakan 1786
Versi kebijakan 1786
Dokumen kebijakan JSON 1786
Pelajari selengkapnya 1787
AWSCleanRoomsFullAccess 1787
Menggunakan kebijakan ini 1787
Rincian kebijakan 1787
Versi kebijakan 1787
Dokumen kebijakan JSON 1788
Pelajari selengkapnya 1792
AWSCleanRoomsFullAccessNoQuerying 1792
Menggunakan kebijakan ini 1792
Rincian kebijakan 1793
Versi kebijakan 1793
Dokumen kebijakan JSON 1793
Pelajari selengkapnya 1798
AWSCleanRoomsMLFullAccess 1798
Menggunakan kebijakan ini 1798
Rincian kebijakan 1798
Versi kebijakan 1798
Dokumen kebijakan JSON 1799
Pelajari selengkapnya 1803
AWSCleanRoomsMLReadOnlyAccess 1803
Menggunakan kebijakan ini 1803
Rincian kebijakan 1803
Versi kebijakan 1803
Dokumen kebijakan JSON 1803
Pelajari selengkapnya 1805
AWSCleanRoomsReadOnlyAccess 1805
Menggunakan kebijakan ini 1805
Rincian kebijakan 1805
Versi kebijakan 1805
Dokumen kebijakan JSON 1805
Pelajari selengkapnya 1807

AWSCloud9Administrator 1807
Menggunakan kebijakan ini 1807
Rincian kebijakan 1807
Versi kebijakan 1807
Dokumen kebijakan JSON 1807
Pelajari selengkapnya 1809
AWSCloud9EnvironmentMember 1809
Menggunakan kebijakan ini 1809
Rincian kebijakan 1809
Versi kebijakan 1810
Dokumen kebijakan JSON 1810
Pelajari selengkapnya 1811
AWSCloud9ServiceRolePolicy 1811
Menggunakan kebijakan ini 1812
Rincian kebijakan 1812
Versi kebijakan 1812
Dokumen kebijakan JSON 1812
Pelajari selengkapnya 1814
AWSCloud9SSMInstanceProfile 1815
Menggunakan kebijakan ini 1815
Rincian kebijakan 1815
Versi kebijakan 1815
Dokumen kebijakan JSON 1815
Pelajari selengkapnya 1816
AWSCloud9User 1816
Menggunakan kebijakan ini 1816
Rincian kebijakan 1816
Versi kebijakan 1816
Dokumen kebijakan JSON 1817
Pelajari selengkapnya 1819
AWSCloudFormationFullAccess 1819
Menggunakan kebijakan ini 1819
Rincian kebijakan 1819
Versi kebijakan 1820
Dokumen kebijakan JSON 1820
Pelajari selengkapnya 1820

AWSCloudFormationReadOnlyAccess 1820
Menggunakan kebijakan ini 1821
Rincian kebijakan 1821
Versi kebijakan 1821
Dokumen kebijakan JSON 1821
Pelajari selengkapnya 1822
AWSCloudFrontLogger 1822
Menggunakan kebijakan ini 1822
Rincian kebijakan 1822
Versi kebijakan 1822
Dokumen kebijakan JSON 1822
Pelajari selengkapnya 1823
AWSCloudFrontVPCOriginServiceRolePolicy 1823
Menggunakan kebijakan ini 1823
Rincian kebijakan 1823
Versi kebijakan 1824
Dokumen kebijakan JSON 1824
Pelajari selengkapnya 1826
AWSCloudHSMFullAccess 1827
Menggunakan kebijakan ini 1827
Rincian kebijakan 1827
Versi kebijakan 1827
Dokumen kebijakan JSON 1827
Pelajari selengkapnya 1828
AWSCloudHSMReadOnlyAccess 1828
Menggunakan kebijakan ini 1828
Rincian kebijakan 1828
Versi kebijakan 1828
Dokumen kebijakan JSON 1828
Pelajari selengkapnya 1829
AWSCloudHSMRole 1829
Menggunakan kebijakan ini 1829
Rincian kebijakan 1829
Versi kebijakan 1829
Dokumen kebijakan JSON 1830
Pelajari selengkapnya 1830

AWSCloudMapDiscoverInstanceAccess 1830
Menggunakan kebijakan ini 1831
Rincian kebijakan 1831
Versi kebijakan 1831
Dokumen kebijakan JSON 1831
Pelajari selengkapnya 1832
AWSCloudMapFullAccess 1832
Menggunakan kebijakan ini 1832
Rincian kebijakan 1832
Versi kebijakan 1832
Dokumen kebijakan JSON 1832
Pelajari selengkapnya 1833
AWSCloudMapReadOnlyAccess 1833
Menggunakan kebijakan ini 1833
Rincian kebijakan 1834
Versi kebijakan 1834
Dokumen kebijakan JSON 1834
Pelajari selengkapnya 1834
AWSCloudMapRegisterInstanceAccess 1835
Menggunakan kebijakan ini 1835
Rincian kebijakan 1835
Versi kebijakan 1835
Dokumen kebijakan JSON 1835
Pelajari selengkapnya 1836
AWSCloudShellFullAccess 1836
Menggunakan kebijakan ini 1836
Rincian kebijakan 1836
Versi kebijakan 1837
Dokumen kebijakan JSON 1837
Pelajari selengkapnya 1837
AWSCloudTrail_FullAccess 1837
Menggunakan kebijakan ini 1838
Rincian kebijakan 1838
Versi kebijakan 1838
Dokumen kebijakan JSON 1838
Pelajari selengkapnya 1841

AWSCloudTrail_ReadOnlyAccess 1841
Menggunakan kebijakan ini 1841
Rincian kebijakan 1841
Versi kebijakan 1841
Dokumen kebijakan JSON 1841
Pelajari selengkapnya 1842
AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy 1842
Menggunakan kebijakan ini 1842
Rincian kebijakan 1842
Versi kebijakan 1843
Dokumen kebijakan JSON 1843
Pelajari selengkapnya 1843
AWSCodeArtifactAdminAccess 1843
Menggunakan kebijakan ini 1844
Rincian kebijakan 1844
Versi kebijakan 1844
Dokumen kebijakan JSON 1844
Pelajari selengkapnya 1845
AWSCodeArtifactReadOnlyAccess 1845
Menggunakan kebijakan ini 1845
Rincian kebijakan 1845
Versi kebijakan 1845
Dokumen kebijakan JSON 1846
Pelajari selengkapnya 1846
AWSCodeBuildAdminAccess 1847
Menggunakan kebijakan ini 1847
Rincian kebijakan 1847
Versi kebijakan 1847
Dokumen kebijakan JSON 1847
Pelajari selengkapnya 1851
AWSCodeBuildDeveloperAccess 1851
Menggunakan kebijakan ini 1851
Rincian kebijakan 1851
Versi kebijakan 1851
Dokumen kebijakan JSON 1851
Pelajari selengkapnya 1854

AWSCodeBuildReadOnlyAccess 1854
Menggunakan kebijakan ini 1854
Rincian kebijakan 1855
Versi kebijakan 1855
Dokumen kebijakan JSON 1855
Pelajari selengkapnya 1856
AWSCodeCommitFullAccess 1857
Menggunakan kebijakan ini 1857
Rincian kebijakan 1857
Versi kebijakan 1857
Dokumen kebijakan JSON 1857
Pelajari selengkapnya 1862
AWSCodeCommitPowerUser 1862
Menggunakan kebijakan ini 1862
Rincian kebijakan 1862
Versi kebijakan 1863
Dokumen kebijakan JSON 1863
Pelajari selengkapnya 1868
AWSCodeCommitReadOnly 1868
Menggunakan kebijakan ini 1868
Rincian kebijakan 1868
Versi kebijakan 1868
Dokumen kebijakan JSON 1868
Pelajari selengkapnya 1871
AWSCodeDeployDeployerAccess 1871
Menggunakan kebijakan ini 1871
Rincian kebijakan 1871
Versi kebijakan 1872
Dokumen kebijakan JSON 1872
Pelajari selengkapnya 1873
AWSCodeDeployFullAccess 1874
Menggunakan kebijakan ini 1874
Rincian kebijakan 1874
Versi kebijakan 1874
Dokumen kebijakan JSON 1874
Pelajari selengkapnya 1876

AWSCodeDeployReadOnlyAccess 1876
Menggunakan kebijakan ini 1876
Rincian kebijakan 1876
Versi kebijakan 1876
Dokumen kebijakan JSON 1877
Pelajari selengkapnya 1878
AWSCodeDeployRole 1878
Menggunakan kebijakan ini 1878
Rincian kebijakan 1878
Versi kebijakan 1878
Dokumen kebijakan JSON 1879
Pelajari selengkapnya 1880
AWSCodeDeployRoleForCloudFormation 1880
Menggunakan kebijakan ini 1880
Rincian kebijakan 1880
Versi kebijakan 1881
Dokumen kebijakan JSON 1881
Pelajari selengkapnya 1881
AWSCodeDeployRoleForECS 1881
Menggunakan kebijakan ini 1882
Rincian kebijakan 1882
Versi kebijakan 1882
Dokumen kebijakan JSON 1882
Pelajari selengkapnya 1883
AWSCodeDeployRoleForECSLimited 1883
Menggunakan kebijakan ini 1883
Rincian kebijakan 1884
Versi kebijakan 1884
Dokumen kebijakan JSON 1884
Pelajari selengkapnya 1886
AWSCodeDeployRoleForLambda 1886
Menggunakan kebijakan ini 1886
Rincian kebijakan 1886
Versi kebijakan 1886
Dokumen kebijakan JSON 1887
Pelajari selengkapnya 1888

AWSCodeDeployRoleForLambdaLimited 1888
Menggunakan kebijakan ini 1888
Rincian kebijakan 1888
Versi kebijakan 1888
Dokumen kebijakan JSON 1889
Pelajari selengkapnya 1890
AWSCodePipeline_FullAccess 1890
Menggunakan kebijakan ini 1890
Rincian kebijakan 1890
Versi kebijakan 1890
Dokumen kebijakan JSON 1891
Pelajari selengkapnya 1894
AWSCodePipeline_ReadOnlyAccess 1894
Menggunakan kebijakan ini 1895
Rincian kebijakan 1895
Versi kebijakan 1895
Dokumen kebijakan JSON 1895
Pelajari selengkapnya 1896
AWSCodePipelineApproverAccess 1897
Menggunakan kebijakan ini 1897
Rincian kebijakan 1897
Versi kebijakan 1897
Dokumen kebijakan JSON 1897
Pelajari selengkapnya 1898
AWSCodePipelineCustomActionAccess 1898
Menggunakan kebijakan ini 1898
Rincian kebijakan 1898
Versi kebijakan 1898
Dokumen kebijakan JSON 1899
Pelajari selengkapnya 1899
AWSCodeStarFullAccess 1899
Menggunakan kebijakan ini 1899
Rincian kebijakan 1900
Versi kebijakan 1900
Dokumen kebijakan JSON 1900
Pelajari selengkapnya 1901

AWSCodeStarNotificationsServiceRolePolicy 1901
Menggunakan kebijakan ini 1901
Rincian kebijakan 1901
Versi kebijakan 1902
Dokumen kebijakan JSON 1902
Pelajari selengkapnya 1903
AWSCodeStarServiceRole 1903
Menggunakan kebijakan ini 1903
Rincian kebijakan 1903
Versi kebijakan 1903
Dokumen kebijakan JSON 1904
Pelajari selengkapnya 1908
AWSCompromisedKeyQuarantine 1909
Menggunakan kebijakan ini 1909
Rincian kebijakan 1909
Versi kebijakan 1909
Dokumen kebijakan JSON 1909
Pelajari selengkapnya 1910
AWSCompromisedKeyQuarantineV2 1911
Menggunakan kebijakan ini 1911
Rincian kebijakan 1911
Versi kebijakan 1911
Dokumen kebijakan JSON 1911
Pelajari selengkapnya 1914
AWSCompromisedKeyQuarantineV3 1914
Menggunakan kebijakan ini 1914
Rincian kebijakan 1914
Versi kebijakan 1915
Dokumen kebijakan JSON 1915
Pelajari selengkapnya 1917
AWSConfigMultiAccountSetupPolicy 1917
Menggunakan kebijakan ini 1918
Rincian kebijakan 1918
Versi kebijakan 1918
Dokumen kebijakan JSON 1918
Pelajari selengkapnya 1920

AWSConfigRemediationServiceRolePolicy 1920
Menggunakan kebijakan ini 1920
Rincian kebijakan 1920
Versi kebijakan 1921
Dokumen kebijakan JSON 1921
Pelajari selengkapnya 1922
AWSConfigRoleForOrganizations 1922
Menggunakan kebijakan ini 1922
Rincian kebijakan 1922
Versi kebijakan 1922
Dokumen kebijakan JSON 1922
Pelajari selengkapnya 1923
AWSConfigRulesExecutionRole 1923
Menggunakan kebijakan ini 1923
Rincian kebijakan 1923
Versi kebijakan 1924
Dokumen kebijakan JSON 1924
Pelajari selengkapnya 1924
AWSConfigServiceRolePolicy 1925
Menggunakan kebijakan ini 1925
Rincian kebijakan 1925
Versi kebijakan 1925
Dokumen kebijakan JSON 1925
Pelajari selengkapnya 1963
AWSConfigUserAccess 1963
Menggunakan kebijakan ini 1963
Rincian kebijakan 1963
Versi kebijakan 1964
Dokumen kebijakan JSON 1964
Pelajari selengkapnya 1964
AWSConnector 1965
Menggunakan kebijakan ini 1965
Rincian kebijakan 1965
Versi kebijakan 1965
Dokumen kebijakan JSON 1965
Pelajari selengkapnya 1967

AWSControlTowerAccountServiceRolePolicy 1967
Menggunakan kebijakan ini 1968
Rincian kebijakan 1968
Versi kebijakan 1968
Dokumen kebijakan JSON 1968
Pelajari selengkapnya 1971
AWSControlTowerServiceRolePolicy 1971
Menggunakan kebijakan ini 1971
Rincian kebijakan 1971
Versi kebijakan 1971
Dokumen kebijakan JSON 1972
Pelajari selengkapnya 1976
AWSCostAndUsageReportAutomationPolicy 1976
Menggunakan kebijakan ini 1977
Rincian kebijakan 1977
Versi kebijakan 1977
Dokumen kebijakan JSON 1977
Pelajari selengkapnya 1978
AWSDataExchangeDataGrantOwnerFullAccess 1978
Menggunakan kebijakan ini 1979
Rincian kebijakan 1979
Versi kebijakan 1979
Dokumen kebijakan JSON 1979
Pelajari selengkapnya 1981
AWSDataExchangeDataGrantReceiverFullAccess 1981
Menggunakan kebijakan ini 1981
Rincian kebijakan 1981
Versi kebijakan 1981
Dokumen kebijakan JSON 1981
Pelajari selengkapnya 1983
AWSDataExchangeFullAccess 1983
Menggunakan kebijakan ini 1983
Rincian kebijakan 1983
Versi kebijakan 1984
Dokumen kebijakan JSON 1984
Pelajari selengkapnya 1987

AWSDataExchangeProviderFullAccess 1988
Menggunakan kebijakan ini 1988
Rincian kebijakan 1988
Versi kebijakan 1988
Dokumen kebijakan JSON 1988
Pelajari selengkapnya 1992
AWSDataExchangeReadOnly 1992
Menggunakan kebijakan ini 1992
Rincian kebijakan 1993
Versi kebijakan 1993
Dokumen kebijakan JSON 1993
Pelajari selengkapnya 1994
AWSDataExchangeServiceRolePolicyForLicenseManagement 1994
Menggunakan kebijakan ini 1995
Rincian kebijakan 1995
Versi kebijakan 1995
Dokumen kebijakan JSON 1995
Pelajari selengkapnya 1996
AWSDataExchangeServiceRolePolicyForOrganizationDiscovery 1996
Menggunakan kebijakan ini 1996
Rincian kebijakan 1996
Versi kebijakan 1996
Dokumen kebijakan JSON 1997
Pelajari selengkapnya 1997
AWSDataExchangeSubscriberFullAccess 1997
Menggunakan kebijakan ini 1997
Rincian kebijakan 1998
Versi kebijakan 1998
Dokumen kebijakan JSON 1998
Pelajari selengkapnya 2000
AWSDataLifecycleManagerServiceRole 2000
Menggunakan kebijakan ini 2001
Rincian kebijakan 2001
Versi kebijakan 2001
Dokumen kebijakan JSON 2001
Pelajari selengkapnya 2002

AWSDataLifecycleManagerServiceRoleForAMIManagement 2003
Menggunakan kebijakan ini 2003
Rincian kebijakan 2003
Versi kebijakan 2003
Dokumen kebijakan JSON 2003
Pelajari selengkapnya 2005
AWSDataLifecycleManagerSSMFullAccess 2005
Menggunakan kebijakan ini 2005
Rincian kebijakan 2005
Versi kebijakan 2005
Dokumen kebijakan JSON 2006
Pelajari selengkapnya 2007
AWSDataPipeline_FullAccess 2007
Menggunakan kebijakan ini 2007
Rincian kebijakan 2007
Versi kebijakan 2008
Dokumen kebijakan JSON 2008
Pelajari selengkapnya 2009
AWSDataPipeline_PowerUser 2009
Menggunakan kebijakan ini 2009
Rincian kebijakan 2009
Versi kebijakan 2009
Dokumen kebijakan JSON 2010
Pelajari selengkapnya 2010
AWSDataSyncDiscoveryServiceRolePolicy 2011
Menggunakan kebijakan ini 2011
Rincian kebijakan 2011
Versi kebijakan 2011
Dokumen kebijakan JSON 2011
Pelajari selengkapnya 2012
AWSDataSyncFullAccess 2013
Menggunakan kebijakan ini 2013
Rincian kebijakan 2013
Versi kebijakan 2013
Dokumen kebijakan JSON 2013
Pelajari selengkapnya 2016

AWSDataSyncReadOnlyAccess 2016
Menggunakan kebijakan ini 2016
Rincian kebijakan 2016
Versi kebijakan 2016
Dokumen kebijakan JSON 2017
Pelajari selengkapnya 2017
AWSDataSyncServiceRolePolicy 2017
Menggunakan kebijakan ini 2018
Rincian kebijakan 2018
Versi kebijakan 2018
Dokumen kebijakan JSON 2018
Pelajari selengkapnya 2019
AWSDeadlineCloud-FleetWorker 2019
Menggunakan kebijakan ini 2020
Rincian kebijakan 2020
Versi kebijakan 2020
Dokumen kebijakan JSON 2020
Pelajari selengkapnya 2021
AWSDeadlineCloud-UserAccessFarms 2021
Menggunakan kebijakan ini 2021
Rincian kebijakan 2021
Versi kebijakan 2021
Dokumen kebijakan JSON 2022
Pelajari selengkapnya 2027
AWSDeadlineCloud-UserAccessFleets 2027
Menggunakan kebijakan ini 2027
Rincian kebijakan 2027
Versi kebijakan 2028
Dokumen kebijakan JSON 2028
Pelajari selengkapnya 2031
AWSDeadlineCloud-UserAccessJobs 2032
Menggunakan kebijakan ini 2032
Rincian kebijakan 2032
Versi kebijakan 2032
Dokumen kebijakan JSON 2032
Pelajari selengkapnya 2036

AWSDeadlineCloud-UserAccessQueues 2036
Menggunakan kebijakan ini 2037
Rincian kebijakan 2037
Versi kebijakan 2037
Dokumen kebijakan JSON 2037
Pelajari selengkapnya 2042
AWSDeadlineCloud-WorkerHost 2042
Menggunakan kebijakan ini 2042
Rincian kebijakan 2042
Versi kebijakan 2042
Dokumen kebijakan JSON 2043
Pelajari selengkapnya 2044
AWSDeepLensLambdaFunctionAccessPolicy 2044
Menggunakan kebijakan ini 2044
Rincian kebijakan 2044
Versi kebijakan 2044
Dokumen kebijakan JSON 2045
Pelajari selengkapnya 2046
AWSDeepLensServiceRolePolicy 2046
Menggunakan kebijakan ini 2046
Rincian kebijakan 2046
Versi kebijakan 2047
Dokumen kebijakan JSON 2047
Pelajari selengkapnya 2054
AWSDeepRacerAccountAdminAccess 2054
Menggunakan kebijakan ini 2054
Rincian kebijakan 2054
Versi kebijakan 2054
Dokumen kebijakan JSON 2055
Pelajari selengkapnya 2055
AWSDeepRacerCloudFormationAccessPolicy 2055
Menggunakan kebijakan ini 2056
Rincian kebijakan 2056
Versi kebijakan 2056
Dokumen kebijakan JSON 2056
Pelajari selengkapnya 2059

AWSDeepRacerDefaultMultiUserAccess 2059
Menggunakan kebijakan ini 2059
Rincian kebijakan 2059
Versi kebijakan 2060
Dokumen kebijakan JSON 2060
Pelajari selengkapnya 2061
AWSDeepRacerFullAccess 2062
Menggunakan kebijakan ini 2062
Rincian kebijakan 2062
Versi kebijakan 2062
Dokumen kebijakan JSON 2062
Pelajari selengkapnya 2063
AWSDeepRacerRoboMakerAccessPolicy 2063
Menggunakan kebijakan ini 2064
Rincian kebijakan 2064
Versi kebijakan 2064
Dokumen kebijakan JSON 2064
Pelajari selengkapnya 2066
AWSDeepRacerServiceRolePolicy 2066
Menggunakan kebijakan ini 2066
Rincian kebijakan 2066
Versi kebijakan 2067
Dokumen kebijakan JSON 2067
Pelajari selengkapnya 2070
AWSDenyAll 2070
Menggunakan kebijakan ini 2070
Rincian kebijakan 2070
Versi kebijakan 2071
Dokumen kebijakan JSON 2071
Pelajari selengkapnya 2071
AWSDeviceFarmFullAccess 2071
Menggunakan kebijakan ini 2072
Rincian kebijakan 2072
Versi kebijakan 2072
Dokumen kebijakan JSON 2072
Pelajari selengkapnya 2072

AWSDeviceFarmServiceRolePolicy 2073
Menggunakan kebijakan ini 2073
Rincian kebijakan 2073
Versi kebijakan 2073
Dokumen kebijakan JSON 2073
Pelajari selengkapnya 2075
AWSDeviceFarmTestGridServiceRolePolicy 2076
Menggunakan kebijakan ini 2076
Rincian kebijakan 2076
Versi kebijakan 2076
Dokumen kebijakan JSON 2076
Pelajari selengkapnya 2078
AWSDirectConnectFullAccess 2079
Menggunakan kebijakan ini 2079
Rincian kebijakan 2079
Versi kebijakan 2079
Dokumen kebijakan JSON 2079
Pelajari selengkapnya 2080
AWSDirectConnectReadOnlyAccess 2080
Menggunakan kebijakan ini 2080
Rincian kebijakan 2080
Versi kebijakan 2080
Dokumen kebijakan JSON 2081
Pelajari selengkapnya 2081
AWSDirectConnectServiceRolePolicy 2081
Menggunakan kebijakan ini 2081
Rincian kebijakan 2082
Versi kebijakan 2082
Dokumen kebijakan JSON 2082
Pelajari selengkapnya 2082
AWSDirectoryServiceDataFullAccess 2083
Menggunakan kebijakan ini 2083
Rincian kebijakan 2083
Versi kebijakan 2083
Dokumen kebijakan JSON 2083
Pelajari selengkapnya 2084

AWSDirectoryServiceDataReadOnlyAccess 2084
Menggunakan kebijakan ini 2084
Rincian kebijakan 2085
Versi kebijakan 2085
Dokumen kebijakan JSON 2085
Pelajari selengkapnya 2086
AWSDirectoryServiceFullAccess 2086
Menggunakan kebijakan ini 2086
Rincian kebijakan 2086
Versi kebijakan 2086
Dokumen kebijakan JSON 2086
Pelajari selengkapnya 2088
AWSDirectoryServiceReadOnlyAccess 2088
Menggunakan kebijakan ini 2089
Rincian kebijakan 2089
Versi kebijakan 2089
Dokumen kebijakan JSON 2089
Pelajari selengkapnya 2090
AWSDiscoveryContinuousExportFirehosePolicy 2090
Menggunakan kebijakan ini 2090
Rincian kebijakan 2090
Versi kebijakan 2091
Dokumen kebijakan JSON 2091
Pelajari selengkapnya 2092
AWSDMSFleetAdvisorServiceRolePolicy 2092
Menggunakan kebijakan ini 2092
Rincian kebijakan 2092
Versi kebijakan 2092
Dokumen kebijakan JSON 2093
Pelajari selengkapnya 2093
AWSDMSServerlessServiceRolePolicy 2093
Menggunakan kebijakan ini 2093
Rincian kebijakan 2094
Versi kebijakan 2094
Dokumen kebijakan JSON 2094
Pelajari selengkapnya 2097

AWSEC2CapacityReservationFleetRolePolicy 2097
Menggunakan kebijakan ini 2097
Rincian kebijakan 2097
Versi kebijakan 2097
Dokumen kebijakan JSON 2098
Pelajari selengkapnya 2099
AWSEC2FleetServiceRolePolicy 2099
Menggunakan kebijakan ini 2099
Rincian kebijakan 2099
Versi kebijakan 2099
Dokumen kebijakan JSON 2100
Pelajari selengkapnya 2102
AWSEC2SpotFleetServiceRolePolicy 2102
Menggunakan kebijakan ini 2102
Rincian kebijakan 2102
Versi kebijakan 2102
Dokumen kebijakan JSON 2102
Pelajari selengkapnya 2104
AWSEC2SpotServiceRolePolicy 2104
Menggunakan kebijakan ini 2105
Rincian kebijakan 2105
Versi kebijakan 2105
Dokumen kebijakan JSON 2105
Pelajari selengkapnya 2107
AWSEC2VssSnapshotPolicy 2107
Menggunakan kebijakan ini 2107
Rincian kebijakan 2107
Versi kebijakan 2107
Dokumen kebijakan JSON 2107
Pelajari selengkapnya 2111
AWSECRPullThroughCache_ServiceRolePolicy 2111
Menggunakan kebijakan ini 2111
Rincian kebijakan 2111
Versi kebijakan 2111
Dokumen kebijakan JSON 2112
Pelajari selengkapnya 2112

AWSElasticBeanstalkCustomPlatformforEC2Role 2113
Menggunakan kebijakan ini 2113
Rincian kebijakan 2113
Versi kebijakan 2113
Dokumen kebijakan JSON 2113
Pelajari selengkapnya 2115
AWSElasticBeanstalkEnhancedHealth 2115
Menggunakan kebijakan ini 2115
Rincian kebijakan 2115
Versi kebijakan 2116
Dokumen kebijakan JSON 2116
Pelajari selengkapnya 2117
AWSElasticBeanstalkMaintenance 2117
Menggunakan kebijakan ini 2117
Rincian kebijakan 2117
Versi kebijakan 2118
Dokumen kebijakan JSON 2118
Pelajari selengkapnya 2119
AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy 2119
Menggunakan kebijakan ini 2119
Rincian kebijakan 2119
Versi kebijakan 2119
Dokumen kebijakan JSON 2120
Pelajari selengkapnya 2127
AWSElasticBeanstalkManagedUpdatesServiceRolePolicy 2127
Menggunakan kebijakan ini 2127
Rincian kebijakan 2127
Versi kebijakan 2127
Dokumen kebijakan JSON 2128
Pelajari selengkapnya 2133
AWSElasticBeanstalkMulticontainerDocker 2133
Menggunakan kebijakan ini 2133
Rincian kebijakan 2133
Versi kebijakan 2134
Dokumen kebijakan JSON 2134
Pelajari selengkapnya 2135

AWSElasticBeanstalkReadOnly 2135
Menggunakan kebijakan ini 2135
Rincian kebijakan 2135
Versi kebijakan 2135
Dokumen kebijakan JSON 2136
Pelajari selengkapnya 2138
AWSElasticBeanstalkRoleCore 2138
Menggunakan kebijakan ini 2138
Rincian kebijakan 2138
Versi kebijakan 2138
Dokumen kebijakan JSON 2139
Pelajari selengkapnya 2143
AWSElasticBeanstalkRoleCWL 2144
Menggunakan kebijakan ini 2144
Rincian kebijakan 2144
Versi kebijakan 2144
Dokumen kebijakan JSON 2144
Pelajari selengkapnya 2145
AWSElasticBeanstalkRoleECS 2145
Menggunakan kebijakan ini 2145
Rincian kebijakan 2145
Versi kebijakan 2145
Dokumen kebijakan JSON 2146
Pelajari selengkapnya 2147
AWSElasticBeanstalkRoleRDS 2147
Menggunakan kebijakan ini 2147
Rincian kebijakan 2147
Versi kebijakan 2147
Dokumen kebijakan JSON 2147
Pelajari selengkapnya 2148
AWSElasticBeanstalkRoleSNS 2148
Menggunakan kebijakan ini 2148
Rincian kebijakan 2149
Versi kebijakan 2149
Dokumen kebijakan JSON 2149
Pelajari selengkapnya 2150

AWSElasticBeanstalkRoleWorkerTier 2150
Menggunakan kebijakan ini 2150
Rincian kebijakan 2150
Versi kebijakan 2150
Dokumen kebijakan JSON 2151
Pelajari selengkapnya 2151
AWSElasticBeanstalkService 2152
Menggunakan kebijakan ini 2152
Rincian kebijakan 2152
Versi kebijakan 2152
Dokumen kebijakan JSON 2152
Pelajari selengkapnya 2157
AWSElasticBeanstalkServiceRolePolicy 2157
Menggunakan kebijakan ini 2157
Rincian kebijakan 2157
Versi kebijakan 2157
Dokumen kebijakan JSON 2158
Pelajari selengkapnya 2159
AWSElasticBeanstalkWebTier 2159
Menggunakan kebijakan ini 2159
Rincian kebijakan 2159
Versi kebijakan 2160
Dokumen kebijakan JSON 2160
Pelajari selengkapnya 2161
AWSElasticBeanstalkWorkerTier 2161
Menggunakan kebijakan ini 2162
Rincian kebijakan 2162
Versi kebijakan 2162
Dokumen kebijakan JSON 2162
Pelajari selengkapnya 2164
AWSElasticDisasterRecoveryAgentInstallationPolicy 2164
Menggunakan kebijakan ini 2165
Rincian kebijakan 2165
Versi kebijakan 2165
Dokumen kebijakan JSON 2165
Pelajari selengkapnya 2167

AWSElasticDisasterRecoveryAgentPolicy 2167
Menggunakan kebijakan ini 2167
Rincian kebijakan 2167
Versi kebijakan 2167
Dokumen kebijakan JSON 2168
Pelajari selengkapnya 2168
AWSElasticDisasterRecoveryConsoleFullAccess 2169
Menggunakan kebijakan ini 2169
Rincian kebijakan 2169
Versi kebijakan 2169
Dokumen kebijakan JSON 2169
Pelajari selengkapnya 2179
AWSElasticDisasterRecoveryConsoleFullAccess_v2 2180
Menggunakan kebijakan ini 2180
Rincian kebijakan 2180
Versi kebijakan 2180
Dokumen kebijakan JSON 2180
Pelajari selengkapnya 2196
AWSElasticDisasterRecoveryConversionServerPolicy 2196
Menggunakan kebijakan ini 2196
Rincian kebijakan 2196
Versi kebijakan 2197
Dokumen kebijakan JSON 2197
Pelajari selengkapnya 2197
AWSElasticDisasterRecoveryCrossAccountReplicationPolicy 2198
Menggunakan kebijakan ini 2198
Rincian kebijakan 2198
Versi kebijakan 2198
Dokumen kebijakan JSON 2198
Pelajari selengkapnya 2199
AWSElasticDisasterRecoveryEc2InstancePolicy 2199
Menggunakan kebijakan ini 2200
Rincian kebijakan 2200
Versi kebijakan 2200
Dokumen kebijakan JSON 2200
Pelajari selengkapnya 2202

AWSElasticDisasterRecoveryFailbackInstallationPolicy 2202
Menggunakan kebijakan ini 2203
Rincian kebijakan 2203
Versi kebijakan 2203
Dokumen kebijakan JSON 2203
Pelajari selengkapnya 2204
AWSElasticDisasterRecoveryFailbackPolicy 2204
Menggunakan kebijakan ini 2204
Rincian kebijakan 2204
Versi kebijakan 2205
Dokumen kebijakan JSON 2205
Pelajari selengkapnya 2206
AWSElasticDisasterRecoveryLaunchActionsPolicy 2206
Menggunakan kebijakan ini 2207
Rincian kebijakan 2207
Versi kebijakan 2207
Dokumen kebijakan JSON 2207
Pelajari selengkapnya 2213
AWSElasticDisasterRecoveryNetworkReplicationPolicy 2213
Menggunakan kebijakan ini 2214
Rincian kebijakan 2214
Versi kebijakan 2214
Dokumen kebijakan JSON 2214
Pelajari selengkapnya 2215
AWSElasticDisasterRecoveryReadOnlyAccess 2215
Menggunakan kebijakan ini 2215
Rincian kebijakan 2215
Versi kebijakan 2216
Dokumen kebijakan JSON 2216
Pelajari selengkapnya 2218
AWSElasticDisasterRecoveryRecoveryInstancePolicy 2218
Menggunakan kebijakan ini 2218
Rincian kebijakan 2218
Versi kebijakan 2219
Dokumen kebijakan JSON 2219
Pelajari selengkapnya 2221

AWSElasticDisasterRecoveryReplicationServerPolicy 2222
Menggunakan kebijakan ini 2222
Rincian kebijakan 2222
Versi kebijakan 2222
Dokumen kebijakan JSON 2223
Pelajari selengkapnya 2225
AWSElasticDisasterRecoveryServiceRolePolicy 2225
Menggunakan kebijakan ini 2225
Rincian kebijakan 2225
Versi kebijakan 2225
Dokumen kebijakan JSON 2226
Pelajari selengkapnya 2236
AWSElasticDisasterRecoveryStagingAccountPolicy 2236
Menggunakan kebijakan ini 2236
Rincian kebijakan 2236
Versi kebijakan 2236
Dokumen kebijakan JSON 2236
Pelajari selengkapnya 2237
AWSElasticDisasterRecoveryStagingAccountPolicy_v2 2238
Menggunakan kebijakan ini 2238
Rincian kebijakan 2238
Versi kebijakan 2238
Dokumen kebijakan JSON 2238
Pelajari selengkapnya 2239
AWSElasticLoadBalancingClassicServiceRolePolicy 2240
Menggunakan kebijakan ini 2240
Rincian kebijakan 2240
Versi kebijakan 2240
Dokumen kebijakan JSON 2240
Pelajari selengkapnya 2241
AWSElasticLoadBalancingServiceRolePolicy 2241
Menggunakan kebijakan ini 2241
Rincian kebijakan 2242
Versi kebijakan 2242
Dokumen kebijakan JSON 2242
Pelajari selengkapnya 2243

AWSElementalMediaConnectFullAccess 2243
Menggunakan kebijakan ini 2243
Rincian kebijakan 2244
Versi kebijakan 2244
Dokumen kebijakan JSON 2244
Pelajari selengkapnya 2244
AWSElementalMediaConnectReadOnlyAccess 2245
Menggunakan kebijakan ini 2245
Rincian kebijakan 2245
Versi kebijakan 2245
Dokumen kebijakan JSON 2245
Pelajari selengkapnya 2246
AWSElementalMediaConvertFullAccess 2246
Menggunakan kebijakan ini 2246
Rincian kebijakan 2246
Versi kebijakan 2247
Dokumen kebijakan JSON 2247
Pelajari selengkapnya 2248
AWSElementalMediaConvertReadOnly 2248
Menggunakan kebijakan ini 2248
Rincian kebijakan 2248
Versi kebijakan 2248
Dokumen kebijakan JSON 2248
Pelajari selengkapnya 2249
AWSElementalMediaLiveFullAccess 2249
Menggunakan kebijakan ini 2249
Rincian kebijakan 2249
Versi kebijakan 2250
Dokumen kebijakan JSON 2250
Pelajari selengkapnya 2250
AWSElementalMediaLiveReadOnly 2250
Menggunakan kebijakan ini 2250
Rincian kebijakan 2251
Versi kebijakan 2251
Dokumen kebijakan JSON 2251
Pelajari selengkapnya 2251

AWSElementalMediaPackageFullAccess 2252
Menggunakan kebijakan ini 2252
Rincian kebijakan 2252
Versi kebijakan 2252
Dokumen kebijakan JSON 2252
Pelajari selengkapnya 2253
AWSElementalMediaPackageReadOnly 2253
Menggunakan kebijakan ini 2253
Rincian kebijakan 2253
Versi kebijakan 2253
Dokumen kebijakan JSON 2253
Pelajari selengkapnya 2254
AWSElementalMediaPackageV2FullAccess 2254
Menggunakan kebijakan ini 2254
Rincian kebijakan 2254
Versi kebijakan 2254
Dokumen kebijakan JSON 2255
Pelajari selengkapnya 2255
AWSElementalMediaPackageV2ReadOnly 2255
Menggunakan kebijakan ini 2255
Rincian kebijakan 2255
Versi kebijakan 2256
Dokumen kebijakan JSON 2256
Pelajari selengkapnya 2256
AWSElementalMediaStoreFullAccess 2256
Menggunakan kebijakan ini 2257
Rincian kebijakan 2257
Versi kebijakan 2257
Dokumen kebijakan JSON 2257
Pelajari selengkapnya 2258
AWSElementalMediaStoreReadOnly 2258
Menggunakan kebijakan ini 2258
Rincian kebijakan 2258
Versi kebijakan 2258
Dokumen kebijakan JSON 2258
Pelajari selengkapnya 2259

AWSElementalMediaTailorFullAccess 2259
Menggunakan kebijakan ini 2259
Rincian kebijakan 2259
Versi kebijakan 2260
Dokumen kebijakan JSON 2260
Pelajari selengkapnya 2260
AWSElementalMediaTailorReadOnly 2260
Menggunakan kebijakan ini 2261
Rincian kebijakan 2261
Versi kebijakan 2261
Dokumen kebijakan JSON 2261
Pelajari selengkapnya 2261
AWSEnhancedClassicNetworkingMangementPolicy 2262
Menggunakan kebijakan ini 2262
Rincian kebijakan 2262
Versi kebijakan 2262
Dokumen kebijakan JSON 2262
Pelajari selengkapnya 2263
AWSEntityResolutionConsoleFullAccess 2263
Menggunakan kebijakan ini 2263
Rincian kebijakan 2263
Versi kebijakan 2263
Dokumen kebijakan JSON 2264
Pelajari selengkapnya 2266
AWSEntityResolutionConsoleReadOnlyAccess 2267
Menggunakan kebijakan ini 2267
Rincian kebijakan 2267
Versi kebijakan 2267
Dokumen kebijakan JSON 2267
Pelajari selengkapnya 2268
AWSFaultInjectionSimulatorEC2Access 2268
Menggunakan kebijakan ini 2268
Rincian kebijakan 2268
Versi kebijakan 2268
Dokumen kebijakan JSON 2269
Pelajari selengkapnya 2270

AWSFaultInjectionSimulatorECSAccess 2270
Menggunakan kebijakan ini 2271
Rincian kebijakan 2271
Versi kebijakan 2271
Dokumen kebijakan JSON 2271
Pelajari selengkapnya 2273
AWSFaultInjectionSimulatorEKSAccess 2273
Menggunakan kebijakan ini 2273
Rincian kebijakan 2273
Versi kebijakan 2274
Dokumen kebijakan JSON 2274
Pelajari selengkapnya 2275
AWSFaultInjectionSimulatorNetworkAccess 2275
Menggunakan kebijakan ini 2275
Rincian kebijakan 2275
Versi kebijakan 2276
Dokumen kebijakan JSON 2276
Pelajari selengkapnya 2283
AWSFaultInjectionSimulatorRDSAccess 2283
Menggunakan kebijakan ini 2283
Rincian kebijakan 2283
Versi kebijakan 2283
Dokumen kebijakan JSON 2284
Pelajari selengkapnya 2285
AWSFaultInjectionSimulatorSSMAccess 2285
Menggunakan kebijakan ini 2285
Rincian kebijakan 2285
Versi kebijakan 2285
Dokumen kebijakan JSON 2286
Pelajari selengkapnya 2287
AWSFinSpaceServiceRolePolicy 2287
Menggunakan kebijakan ini 2287
Rincian kebijakan 2287
Versi kebijakan 2288
Dokumen kebijakan JSON 2288
Pelajari selengkapnya 2288

AWSFMAdminFullAccess 2289
Menggunakan kebijakan ini 2289
Rincian kebijakan 2289
Versi kebijakan 2289
Dokumen kebijakan JSON 2289
Pelajari selengkapnya 2291
AWSFMAdminReadOnlyAccess 2291
Menggunakan kebijakan ini 2291
Rincian kebijakan 2291
Versi kebijakan 2292
Dokumen kebijakan JSON 2292
Pelajari selengkapnya 2293
AWSFMMemberReadOnlyAccess 2294
Menggunakan kebijakan ini 2294
Rincian kebijakan 2294
Versi kebijakan 2294
Dokumen kebijakan JSON 2294
Pelajari selengkapnya 2295
AWSForWordPressPluginPolicy 2295
Menggunakan kebijakan ini 2295
Rincian kebijakan 2295
Versi kebijakan 2295
Dokumen kebijakan JSON 2296
Pelajari selengkapnya 2297
AWSGitSyncServiceRolePolicy 2298
Menggunakan kebijakan ini 2298
Rincian kebijakan 2298
Versi kebijakan 2298
Dokumen kebijakan JSON 2298
Pelajari selengkapnya 2299
AWSGlobalAcceleratorSLRPolicy 2299
Menggunakan kebijakan ini 2299
Rincian kebijakan 2299
Versi kebijakan 2300
Dokumen kebijakan JSON 2300
Pelajari selengkapnya 2301

AWSGlueConsoleFullAccess 2301
Menggunakan kebijakan ini 2302
Rincian kebijakan 2302
Versi kebijakan 2302
Dokumen kebijakan JSON 2302
Pelajari selengkapnya 2306
AWSGlueConsoleSageMakerNotebookFullAccess 2306
Menggunakan kebijakan ini 2307
Rincian kebijakan 2307
Versi kebijakan 2307
Dokumen kebijakan JSON 2307
Pelajari selengkapnya 2312
AwsGlueDataBrewFullAccessPolicy 2313
Menggunakan kebijakan ini 2313
Rincian kebijakan 2313
Versi kebijakan 2313
Dokumen kebijakan JSON 2313
Pelajari selengkapnya 2318
AWSGlueDataBrewServiceRole 2319
Menggunakan kebijakan ini 2319
Rincian kebijakan 2319
Versi kebijakan 2319
Dokumen kebijakan JSON 2319
Pelajari selengkapnya 2322
AWSGlueSchemaRegistryFullAccess 2322
Menggunakan kebijakan ini 2322
Rincian kebijakan 2323
Versi kebijakan 2323
Dokumen kebijakan JSON 2323
Pelajari selengkapnya 2324
AWSGlueSchemaRegistryReadonlyAccess 2324
Menggunakan kebijakan ini 2325
Rincian kebijakan 2325
Versi kebijakan 2325
Dokumen kebijakan JSON 2325
Pelajari selengkapnya 2326

AWSGlueServiceNotebookRole 2326
Menggunakan kebijakan ini 2326
Rincian kebijakan 2326
Versi kebijakan 2326
Dokumen kebijakan JSON 2327
Pelajari selengkapnya 2329
AWSGlueServiceRole 2329
Menggunakan kebijakan ini 2329
Rincian kebijakan 2329
Versi kebijakan 2330
Dokumen kebijakan JSON 2330
Pelajari selengkapnya 2332
AwsGlueSessionUserRestrictedNotebookPolicy 2332
Menggunakan kebijakan ini 2332
Rincian kebijakan 2333
Versi kebijakan 2333
Dokumen kebijakan JSON 2333
Pelajari selengkapnya 2336
AwsGlueSessionUserRestrictedNotebookServiceRole 2336
Menggunakan kebijakan ini 2336
Rincian kebijakan 2336
Versi kebijakan 2337
Dokumen kebijakan JSON 2337
Pelajari selengkapnya 2341
AwsGlueSessionUserRestrictedPolicy 2341
Menggunakan kebijakan ini 2341
Rincian kebijakan 2341
Versi kebijakan 2341
Dokumen kebijakan JSON 2342
Pelajari selengkapnya 2344
AwsGlueSessionUserRestrictedServiceRole 2345
Menggunakan kebijakan ini 2345
Rincian kebijakan 2345
Versi kebijakan 2345
Dokumen kebijakan JSON 2345
Pelajari selengkapnya 2350

AWSGrafanaAccountAdministrator 2350
Menggunakan kebijakan ini 2350
Rincian kebijakan 2350
Versi kebijakan 2350
Dokumen kebijakan JSON 2351
Pelajari selengkapnya 2352
AWSGrafanaConsoleReadOnlyAccess 2352
Menggunakan kebijakan ini 2352
Rincian kebijakan 2352
Versi kebijakan 2352
Dokumen kebijakan JSON 2352
Pelajari selengkapnya 2353
AWSGrafanaWorkspacePermissionManagement 2353
Menggunakan kebijakan ini 2353
Rincian kebijakan 2353
Versi kebijakan 2354
Dokumen kebijakan JSON 2354
Pelajari selengkapnya 2355
AWSGrafanaWorkspacePermissionManagementV2 2355
Menggunakan kebijakan ini 2355
Rincian kebijakan 2355
Versi kebijakan 2355
Dokumen kebijakan JSON 2356
Pelajari selengkapnya 2356
AWSGreengrassFullAccess 2357
Menggunakan kebijakan ini 2357
Rincian kebijakan 2357
Versi kebijakan 2357
Dokumen kebijakan JSON 2357
Pelajari selengkapnya 2358
AWSGreengrassReadOnlyAccess 2358
Menggunakan kebijakan ini 2358
Rincian kebijakan 2358
Versi kebijakan 2358
Dokumen kebijakan JSON 2359
Pelajari selengkapnya 2359

AWSGreengrassResourceAccessRolePolicy 2359
Menggunakan kebijakan ini 2359
Rincian kebijakan 2359
Versi kebijakan 2360
Dokumen kebijakan JSON 2360
Pelajari selengkapnya 2362
AWSGroundStationAgentInstancePolicy 2362
Menggunakan kebijakan ini 2363
Rincian kebijakan 2363
Versi kebijakan 2363
Dokumen kebijakan JSON 2363
Pelajari selengkapnya 2364
AWSHealth_EventProcessorServiceRolePolicy 2364
Menggunakan kebijakan ini 2364
Rincian kebijakan 2364
Versi kebijakan 2364
Dokumen kebijakan JSON 2365
Pelajari selengkapnya 2365
AWSHealthFullAccess 2365
Menggunakan kebijakan ini 2366
Rincian kebijakan 2366
Versi kebijakan 2366
Dokumen kebijakan JSON 2366
Pelajari selengkapnya 2367
AWSHealthImagingFullAccess 2367
Menggunakan kebijakan ini 2367
Rincian kebijakan 2368
Versi kebijakan 2368
Dokumen kebijakan JSON 2368
Pelajari selengkapnya 2369
AWSHealthImagingReadOnlyAccess 2369
Menggunakan kebijakan ini 2369
Rincian kebijakan 2369
Versi kebijakan 2369
Dokumen kebijakan JSON 2369
Pelajari selengkapnya 2370

AWSIAMIdentityCenterAllowListForIdentityContext 2370
Menggunakan kebijakan ini 2370
Rincian kebijakan 2371
Versi kebijakan 2371
Dokumen kebijakan JSON 2371
Pelajari selengkapnya 2374
AWSIdentitySyncFullAccess 2374
Menggunakan kebijakan ini 2374
Rincian kebijakan 2375
Versi kebijakan 2375
Dokumen kebijakan JSON 2375
Pelajari selengkapnya 2376
AWSIdentitySyncReadOnlyAccess 2376
Menggunakan kebijakan ini 2376
Rincian kebijakan 2376
Versi kebijakan 2376
Dokumen kebijakan JSON 2377
Pelajari selengkapnya 2377
AWSImageBuilderFullAccess 2377
Menggunakan kebijakan ini 2377
Rincian kebijakan 2378
Versi kebijakan 2378
Dokumen kebijakan JSON 2378
Pelajari selengkapnya 2381
AWSImageBuilderReadOnlyAccess 2381
Menggunakan kebijakan ini 2381
Rincian kebijakan 2381
Versi kebijakan 2381
Dokumen kebijakan JSON 2382
Pelajari selengkapnya 2382
AWSImportExportFullAccess 2382
Menggunakan kebijakan ini 2382
Rincian kebijakan 2383
Versi kebijakan 2383
Dokumen kebijakan JSON 2383
Pelajari selengkapnya 2383

AWSImportExportReadOnlyAccess 2384
Menggunakan kebijakan ini 2384
Rincian kebijakan 2384
Versi kebijakan 2384
Dokumen kebijakan JSON 2384
Pelajari selengkapnya 2385
AWSIncidentManagerIncidentAccessServiceRolePolicy 2385
Menggunakan kebijakan ini 2385
Rincian kebijakan 2385
Versi kebijakan 2385
Dokumen kebijakan JSON 2386
Pelajari selengkapnya 2386
AWSIncidentManagerResolverAccess 2386
Menggunakan kebijakan ini 2387
Rincian kebijakan 2387
Versi kebijakan 2387
Dokumen kebijakan JSON 2387
Pelajari selengkapnya 2388
AWSIncidentManagerServiceRolePolicy 2388
Menggunakan kebijakan ini 2389
Rincian kebijakan 2389
Versi kebijakan 2389
Dokumen kebijakan JSON 2389
Pelajari selengkapnya 2390
AWSIoT1ClickFullAccess 2390
Menggunakan kebijakan ini 2391
Rincian kebijakan 2391
Versi kebijakan 2391
Dokumen kebijakan JSON 2391
Pelajari selengkapnya 2391
AWSIoT1ClickReadOnlyAccess 2392
Menggunakan kebijakan ini 2392
Rincian kebijakan 2392
Versi kebijakan 2392
Dokumen kebijakan JSON 2392
Pelajari selengkapnya 2393

AWSIoTAnalyticsFullAccess 2393
Menggunakan kebijakan ini 2393
Rincian kebijakan 2393
Versi kebijakan 2393
Dokumen kebijakan JSON 2394
Pelajari selengkapnya 2394
AWSIoTAnalyticsReadOnlyAccess 2394
Menggunakan kebijakan ini 2394
Rincian kebijakan 2394
Versi kebijakan 2395
Dokumen kebijakan JSON 2395
Pelajari selengkapnya 2395
AWSIoTConfigAccess 2395
Menggunakan kebijakan ini 2396
Rincian kebijakan 2396
Versi kebijakan 2396
Dokumen kebijakan JSON 2396
Pelajari selengkapnya 2400
AWSIoTConfigReadOnlyAccess 2400
Menggunakan kebijakan ini 2400
Rincian kebijakan 2400
Versi kebijakan 2401
Dokumen kebijakan JSON 2401
Pelajari selengkapnya 2403
AWSIoTDataAccess 2403
Menggunakan kebijakan ini 2403
Rincian kebijakan 2403
Versi kebijakan 2403
Dokumen kebijakan JSON 2404
Pelajari selengkapnya 2404
AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction 2404
Menggunakan kebijakan ini 2405
Rincian kebijakan 2405
Versi kebijakan 2405
Dokumen kebijakan JSON 2405
Pelajari selengkapnya 2406

AWSIoTDeviceDefenderAudit 2406
Menggunakan kebijakan ini 2406
Rincian kebijakan 2406
Versi kebijakan 2406
Dokumen kebijakan JSON 2406
Pelajari selengkapnya 2407
AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction 2408
Menggunakan kebijakan ini 2408
Rincian kebijakan 2408
Versi kebijakan 2408
Dokumen kebijakan JSON 2408
Pelajari selengkapnya 2409
AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction 2409
Menggunakan kebijakan ini 2410
Rincian kebijakan 2410
Versi kebijakan 2410
Dokumen kebijakan JSON 2410
Pelajari selengkapnya 2411
AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction 2411
Menggunakan kebijakan ini 2411
Rincian kebijakan 2411
Versi kebijakan 2411
Dokumen kebijakan JSON 2412
Pelajari selengkapnya 2412
AWSIoTDeviceDefenderUpdateCACertMitigationAction 2412
Menggunakan kebijakan ini 2412
Rincian kebijakan 2413
Versi kebijakan 2413
Dokumen kebijakan JSON 2413
Pelajari selengkapnya 2413
AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction 2414
Menggunakan kebijakan ini 2414
Rincian kebijakan 2414
Versi kebijakan 2414
Dokumen kebijakan JSON 2414
Pelajari selengkapnya 2415

AWSIoTDeviceTesterForFreeRTOSFullAccess 2415
Menggunakan kebijakan ini 2415
Rincian kebijakan 2415
Versi kebijakan 2416
Dokumen kebijakan JSON 2416
Pelajari selengkapnya 2422
AWSIoTDeviceTesterForGreengrassFullAccess 2422
Menggunakan kebijakan ini 2422
Rincian kebijakan 2422
Versi kebijakan 2423
Dokumen kebijakan JSON 2423
Pelajari selengkapnya 2426
AWSIoTEventsFullAccess 2426
Menggunakan kebijakan ini 2426
Rincian kebijakan 2426
Versi kebijakan 2426
Dokumen kebijakan JSON 2426
Pelajari selengkapnya 2427
AWSIoTEventsReadOnlyAccess 2427
Menggunakan kebijakan ini 2427
Rincian kebijakan 2427
Versi kebijakan 2428
Dokumen kebijakan JSON 2428
Pelajari selengkapnya 2428
AWSIoTFleetHubFederationAccess 2428
Menggunakan kebijakan ini 2429
Rincian kebijakan 2429
Versi kebijakan 2429
Dokumen kebijakan JSON 2429
Pelajari selengkapnya 2431
AWSIoTFleetwiseServiceRolePolicy 2431
Menggunakan kebijakan ini 2431
Rincian kebijakan 2431
Versi kebijakan 2432
Dokumen kebijakan JSON 2432
Pelajari selengkapnya 2432

AWSIoTFullAccess 2432
Menggunakan kebijakan ini 2433
Rincian kebijakan 2433
Versi kebijakan 2433
Dokumen kebijakan JSON 2433
Pelajari selengkapnya 2433
AWSIoTLogging 2434
Menggunakan kebijakan ini 2434
Rincian kebijakan 2434
Versi kebijakan 2434
Dokumen kebijakan JSON 2434
Pelajari selengkapnya 2435
AWSIoTManagedIntegrationsFullAccess 2435
Menggunakan kebijakan ini 2435
Rincian kebijakan 2435
Versi kebijakan 2436
Dokumen kebijakan JSON 2436
Pelajari selengkapnya 2436
AWSIoTManagedIntegrationsRolePolicy 2437
Menggunakan kebijakan ini 2437
Rincian kebijakan 2437
Versi kebijakan 2437
Dokumen kebijakan JSON 2437
Pelajari selengkapnya 2439
AWSIoTOTAUpdate 2439
Menggunakan kebijakan ini 2439
Rincian kebijakan 2439
Versi kebijakan 2439
Dokumen kebijakan JSON 2439
Pelajari selengkapnya 2440
AWSIotRoboRunnerFullAccess 2440
Menggunakan kebijakan ini 2440
Rincian kebijakan 2440
Versi kebijakan 2440
Dokumen kebijakan JSON 2441
Pelajari selengkapnya 2441

AWSIotRoboRunnerReadOnly 2441
Menggunakan kebijakan ini 2442
Rincian kebijakan 2442
Versi kebijakan 2442
Dokumen kebijakan JSON 2442
Pelajari selengkapnya 2443
AWSIotRoboRunnerServiceRolePolicy 2443
Menggunakan kebijakan ini 2443
Rincian kebijakan 2443
Versi kebijakan 2443
Dokumen kebijakan JSON 2444
Pelajari selengkapnya 2444
AWSIoTRuleActions 2444
Menggunakan kebijakan ini 2444
Rincian kebijakan 2445
Versi kebijakan 2445
Dokumen kebijakan JSON 2445
Pelajari selengkapnya 2445
AWSIoTSiteWiseConsoleFullAccess 2446
Menggunakan kebijakan ini 2446
Rincian kebijakan 2446
Versi kebijakan 2446
Dokumen kebijakan JSON 2447
Pelajari selengkapnya 2449
AWSIoTSiteWiseFullAccess 2449
Menggunakan kebijakan ini 2449
Rincian kebijakan 2449
Versi kebijakan 2449
Dokumen kebijakan JSON 2449
Pelajari selengkapnya 2450
AWSIoTSiteWiseMonitorPortalAccess 2450
Menggunakan kebijakan ini 2450
Rincian kebijakan 2450
Versi kebijakan 2451
Dokumen kebijakan JSON 2451
Pelajari selengkapnya 2452

AWSIoTSiteWiseMonitorServiceRolePolicy 2452
Menggunakan kebijakan ini 2452
Rincian kebijakan 2452
Versi kebijakan 2452
Dokumen kebijakan JSON 2453
Pelajari selengkapnya 2454
AWSIoTSiteWiseReadOnlyAccess 2454
Menggunakan kebijakan ini 2454
Rincian kebijakan 2454
Versi kebijakan 2454
Dokumen kebijakan JSON 2454
Pelajari selengkapnya 2455
AWSIoTThingsRegistration 2455
Menggunakan kebijakan ini 2455
Rincian kebijakan 2455
Versi kebijakan 2456
Dokumen kebijakan JSON 2456
Pelajari selengkapnya 2457
AWSIoTTwinMakerServiceRolePolicy 2457
Menggunakan kebijakan ini 2457
Rincian kebijakan 2457
Versi kebijakan 2458
Dokumen kebijakan JSON 2458
Pelajari selengkapnya 2459
AWSIoTWirelessDataAccess 2459
Menggunakan kebijakan ini 2460
Rincian kebijakan 2460
Versi kebijakan 2460
Dokumen kebijakan JSON 2460
Pelajari selengkapnya 2460
AWSIoTWirelessFullAccess 2461
Menggunakan kebijakan ini 2461
Rincian kebijakan 2461
Versi kebijakan 2461
Dokumen kebijakan JSON 2461
Pelajari selengkapnya 2462

AWSIoTWirelessFullPublishAccess 2462
Menggunakan kebijakan ini 2462
Rincian kebijakan 2462
Versi kebijakan 2462
Dokumen kebijakan JSON 2463
Pelajari selengkapnya 2463
AWSIoTWirelessGatewayCertManager 2463
Menggunakan kebijakan ini 2463
Rincian kebijakan 2464
Versi kebijakan 2464
Dokumen kebijakan JSON 2464
Pelajari selengkapnya 2464
AWSIoTWirelessLogging 2465
Menggunakan kebijakan ini 2465
Rincian kebijakan 2465
Versi kebijakan 2465
Dokumen kebijakan JSON 2465
Pelajari selengkapnya 2466
AWSIoTWirelessReadOnlyAccess 2466
Menggunakan kebijakan ini 2466
Rincian kebijakan 2466
Versi kebijakan 2466
Dokumen kebijakan JSON 2467
Pelajari selengkapnya 2467
AWSIPAMServiceRolePolicy 2467
Menggunakan kebijakan ini 2467
Rincian kebijakan 2468
Versi kebijakan 2468
Dokumen kebijakan JSON 2468
Pelajari selengkapnya 2469
AWSIQContractServiceRolePolicy 2469
Menggunakan kebijakan ini 2469
Rincian kebijakan 2470
Versi kebijakan 2470
Dokumen kebijakan JSON 2470
Pelajari selengkapnya 2470

AWSIQFullAccess 2471
Menggunakan kebijakan ini 2471
Rincian kebijakan 2471
Versi kebijakan 2471
Dokumen kebijakan JSON 2471
Pelajari selengkapnya 2472
AWSIQPermissionServiceRolePolicy 2472
Menggunakan kebijakan ini 2472
Rincian kebijakan 2472
Versi kebijakan 2473
Dokumen kebijakan JSON 2473
Pelajari selengkapnya 2474
AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy 2474
Menggunakan kebijakan ini 2474
Rincian kebijakan 2474
Versi kebijakan 2474
Dokumen kebijakan JSON 2475
Pelajari selengkapnya 2475
AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy 2475
Menggunakan kebijakan ini 2476
Rincian kebijakan 2476
Versi kebijakan 2476
Dokumen kebijakan JSON 2476
Pelajari selengkapnya 2477
AWSKeyManagementServicePowerUser 2477
Menggunakan kebijakan ini 2477
Rincian kebijakan 2477
Versi kebijakan 2477
Dokumen kebijakan JSON 2477
Pelajari selengkapnya 2478
AWSLakeFormationCrossAccountManager 2478
Menggunakan kebijakan ini 2478
Rincian kebijakan 2479
Versi kebijakan 2479
Dokumen kebijakan JSON 2479
Pelajari selengkapnya 2481

AWSLakeFormationDataAdmin 2481
Menggunakan kebijakan ini 2481
Rincian kebijakan 2481
Versi kebijakan 2482
Dokumen kebijakan JSON 2482
Pelajari selengkapnya 2483
AWSLambda_FullAccess 2483
Menggunakan kebijakan ini 2484
Rincian kebijakan 2484
Versi kebijakan 2484
Dokumen kebijakan JSON 2484
Pelajari selengkapnya 2485
AWSLambda_ReadOnlyAccess 2486
Menggunakan kebijakan ini 2486
Rincian kebijakan 2486
Versi kebijakan 2486
Dokumen kebijakan JSON 2486
Pelajari selengkapnya 2488
AWSLambdaBasicExecutionRole 2488
Menggunakan kebijakan ini 2488
Rincian kebijakan 2488
Versi kebijakan 2488
Dokumen kebijakan JSON 2488
Pelajari selengkapnya 2489
AWSLambdaDynamoDBExecutionRole 2489
Menggunakan kebijakan ini 2489
Rincian kebijakan 2489
Versi kebijakan 2490
Dokumen kebijakan JSON 2490
Pelajari selengkapnya 2490
AWSLambdaENIManagementAccess 2491
Menggunakan kebijakan ini 2491
Rincian kebijakan 2491
Versi kebijakan 2491
Dokumen kebijakan JSON 2491
Pelajari selengkapnya 2492

AWSLambdaExecute 2492
Menggunakan kebijakan ini 2492
Rincian kebijakan 2492
Versi kebijakan 2492
Dokumen kebijakan JSON 2493
Pelajari selengkapnya 2493
AWSLambdaFullAccess 2493
Menggunakan kebijakan ini 2494
Rincian kebijakan 2494
Versi kebijakan 2494
Dokumen kebijakan JSON 2494
Pelajari selengkapnya 2496
AWSLambdaInvocation-DynamoDB 2496
Menggunakan kebijakan ini 2496
Rincian kebijakan 2496
Versi kebijakan 2496
Dokumen kebijakan JSON 2496
Pelajari selengkapnya 2497
AWSLambdaKinesisExecutionRole 2497
Menggunakan kebijakan ini 2497
Rincian kebijakan 2498
Versi kebijakan 2498
Dokumen kebijakan JSON 2498
Pelajari selengkapnya 2499
AWSLambdaMSKExecutionRole 2499
Menggunakan kebijakan ini 2499
Rincian kebijakan 2499
Versi kebijakan 2499
Dokumen kebijakan JSON 2499
Pelajari selengkapnya 2500
AWSLambdaReplicator 2500
Menggunakan kebijakan ini 2501
Rincian kebijakan 2501
Versi kebijakan 2501
Dokumen kebijakan JSON 2501
Pelajari selengkapnya 2502

AWSLambdaRole 2502
Menggunakan kebijakan ini 2502
Rincian kebijakan 2503
Versi kebijakan 2503
Dokumen kebijakan JSON 2503
Pelajari selengkapnya 2503
AWSLambdaSQSQueueExecutionRole 2504
Menggunakan kebijakan ini 2504
Rincian kebijakan 2504
Versi kebijakan 2504
Dokumen kebijakan JSON 2504
Pelajari selengkapnya 2505
AWSLambdaVPCAccessExecutionRole 2505
Menggunakan kebijakan ini 2505
Rincian kebijakan 2505
Versi kebijakan 2506
Dokumen kebijakan JSON 2506
Pelajari selengkapnya 2506
AWSLicenseManagerConsumptionPolicy 2507
Menggunakan kebijakan ini 2507
Rincian kebijakan 2507
Versi kebijakan 2507
Dokumen kebijakan JSON 2507
Pelajari selengkapnya 2508
AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy 2508
Menggunakan kebijakan ini 2508
Rincian kebijakan 2508
Versi kebijakan 2508
Dokumen kebijakan JSON 2509
Pelajari selengkapnya 2510
AWSLicenseManagerMasterAccountRolePolicy 2511
Menggunakan kebijakan ini 2511
Rincian kebijakan 2511
Versi kebijakan 2511
Dokumen kebijakan JSON 2511
Pelajari selengkapnya 2516

AWSLicenseManagerMemberAccountRolePolicy 2516
Menggunakan kebijakan ini 2516
Rincian kebijakan 2517
Versi kebijakan 2517
Dokumen kebijakan JSON 2517
Pelajari selengkapnya 2518
AWSLicenseManagerServiceRolePolicy 2518
Menggunakan kebijakan ini 2518
Rincian kebijakan 2519
Versi kebijakan 2519
Dokumen kebijakan JSON 2519
Pelajari selengkapnya 2522
AWSLicenseManagerUserSubscriptionsServiceRolePolicy 2522
Menggunakan kebijakan ini 2523
Rincian kebijakan 2523
Versi kebijakan 2523
Dokumen kebijakan JSON 2523
Pelajari selengkapnya 2526
AWSM2ServicePolicy 2526
Menggunakan kebijakan ini 2526
Rincian kebijakan 2526
Versi kebijakan 2527
Dokumen kebijakan JSON 2527
Pelajari selengkapnya 2528
AWSManagedServices_ContactsServiceRolePolicy 2528
Menggunakan kebijakan ini 2529
Rincian kebijakan 2529
Versi kebijakan 2529
Dokumen kebijakan JSON 2529
Pelajari selengkapnya 2530
AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy 2530
Menggunakan kebijakan ini 2530
Rincian kebijakan 2530
Versi kebijakan 2531
Dokumen kebijakan JSON 2531
Pelajari selengkapnya 2532

AWSManagedServices_EventsServiceRolePolicy 2532
Menggunakan kebijakan ini 2533
Rincian kebijakan 2533
Versi kebijakan 2533
Dokumen kebijakan JSON 2533
Pelajari selengkapnya 2534
AWSManagedServices_SelfServiceReporting_ServiceRolePolicy 2534
Menggunakan kebijakan ini 2534
Rincian kebijakan 2534
Versi kebijakan 2535
Dokumen kebijakan JSON 2535
Pelajari selengkapnya 2535
AWSManagedServicesDeploymentToolkitPolicy 2535
Menggunakan kebijakan ini 2536
Rincian kebijakan 2536
Versi kebijakan 2536
Dokumen kebijakan JSON 2536
Pelajari selengkapnya 2538
AWSMarketplaceAmiIngestion 2538
Menggunakan kebijakan ini 2539
Rincian kebijakan 2539
Versi kebijakan 2539
Dokumen kebijakan JSON 2539
Pelajari selengkapnya 2540
AWSMarketplaceDeploymentServiceRolePolicy 2540
Menggunakan kebijakan ini 2540
Rincian kebijakan 2540
Versi kebijakan 2540
Dokumen kebijakan JSON 2541
Pelajari selengkapnya 2542
AWSMarketplaceFullAccess 2542
Menggunakan kebijakan ini 2542
Rincian kebijakan 2542
Versi kebijakan 2543
Dokumen kebijakan JSON 2543
Pelajari selengkapnya 2545

AWSMarketplaceGetEntitlements 2545
Menggunakan kebijakan ini 2545
Rincian kebijakan 2545
Versi kebijakan 2545
Dokumen kebijakan JSON 2546
Pelajari selengkapnya 2546
AWSMarketplaceImageBuildFullAccess 2546
Menggunakan kebijakan ini 2546
Rincian kebijakan 2546
Versi kebijakan 2547
Dokumen kebijakan JSON 2547
Pelajari selengkapnya 2550
AWSMarketplaceLicenseManagementServiceRolePolicy 2551
Menggunakan kebijakan ini 2551
Rincian kebijakan 2551
Versi kebijakan 2551
Dokumen kebijakan JSON 2551
Pelajari selengkapnya 2552
AWSMarketplaceManageSubscriptions 2552
Menggunakan kebijakan ini 2552
Rincian kebijakan 2552
Versi kebijakan 2553
Dokumen kebijakan JSON 2553
Pelajari selengkapnya 2554
AWSMarketplaceMeteringFullAccess 2554
Menggunakan kebijakan ini 2554
Rincian kebijakan 2554
Versi kebijakan 2555
Dokumen kebijakan JSON 2555
Pelajari selengkapnya 2555
AWSMarketplaceMeteringRegisterUsage 2555
Menggunakan kebijakan ini 2556
Rincian kebijakan 2556
Versi kebijakan 2556
Dokumen kebijakan JSON 2556
Pelajari selengkapnya 2556

AWSMarketplaceProcurementSystemAdminFullAccess 2557
Menggunakan kebijakan ini 2557
Rincian kebijakan 2557
Versi kebijakan 2557
Dokumen kebijakan JSON 2557
Pelajari selengkapnya 2558
AWSMarketplacePurchaseOrdersServiceRolePolicy 2558
Menggunakan kebijakan ini 2558
Rincian kebijakan 2558
Versi kebijakan 2559
Dokumen kebijakan JSON 2559
Pelajari selengkapnya 2559
AWSMarketplaceRead-only 2559
Menggunakan kebijakan ini 2560
Rincian kebijakan 2560
Versi kebijakan 2560
Dokumen kebijakan JSON 2560
Pelajari selengkapnya 2561
AWSMarketplaceResaleAuthorizationServiceRolePolicy 2561
Menggunakan kebijakan ini 2562
Rincian kebijakan 2562
Versi kebijakan 2562
Dokumen kebijakan JSON 2562
Pelajari selengkapnya 2564
AWSMarketplaceSellerFullAccess 2565
Menggunakan kebijakan ini 2565
Rincian kebijakan 2565
Versi kebijakan 2565
Dokumen kebijakan JSON 2565
Pelajari selengkapnya 2569
AWSMarketplaceSellerOfferManagement 2569
Menggunakan kebijakan ini 2569
Rincian kebijakan 2569
Versi kebijakan 2569
Dokumen kebijakan JSON 2570
Pelajari selengkapnya 2572

AWSMarketplaceSellerProductsFullAccess 2572
Menggunakan kebijakan ini 2572
Rincian kebijakan 2572
Versi kebijakan 2572
Dokumen kebijakan JSON 2572
Pelajari selengkapnya 2574
AWSMarketplaceSellerProductsReadOnly 2574
Menggunakan kebijakan ini 2575
Rincian kebijakan 2575
Versi kebijakan 2575
Dokumen kebijakan JSON 2575
Pelajari selengkapnya 2576
AWSMediaConnectServicePolicy 2576
Menggunakan kebijakan ini 2576
Rincian kebijakan 2576
Versi kebijakan 2577
Dokumen kebijakan JSON 2577
Pelajari selengkapnya 2578
AWSMediaLiveAnywhereServiceRolePolicy 2578
Menggunakan kebijakan ini 2578
Rincian kebijakan 2579
Versi kebijakan 2579
Dokumen kebijakan JSON 2579
Pelajari selengkapnya 2582
AWSMediaTailorServiceRolePolicy 2582
Menggunakan kebijakan ini 2582
Rincian kebijakan 2582
Versi kebijakan 2583
Dokumen kebijakan JSON 2583
Pelajari selengkapnya 2583
AWSMigrationHubDiscoveryAccess 2583
Menggunakan kebijakan ini 2584
Rincian kebijakan 2584
Versi kebijakan 2584
Dokumen kebijakan JSON 2584
Pelajari selengkapnya 2585

AWSMigrationHubDMSAccess 2586
Menggunakan kebijakan ini 2586
Rincian kebijakan 2586
Versi kebijakan 2586
Dokumen kebijakan JSON 2586
Pelajari selengkapnya 2587
AWSMigrationHubFullAccess 2587
Menggunakan kebijakan ini 2588
Rincian kebijakan 2588
Versi kebijakan 2588
Dokumen kebijakan JSON 2588
Pelajari selengkapnya 2589
AWSMigrationHubOrchestratorConsoleFullAccess 2590
Menggunakan kebijakan ini 2590
Rincian kebijakan 2590
Versi kebijakan 2590
Dokumen kebijakan JSON 2590
Pelajari selengkapnya 2593
AWSMigrationHubOrchestratorInstanceRolePolicy 2594
Menggunakan kebijakan ini 2594
Rincian kebijakan 2594
Versi kebijakan 2594
Dokumen kebijakan JSON 2594
Pelajari selengkapnya 2595
AWSMigrationHubOrchestratorPlugin 2595
Menggunakan kebijakan ini 2595
Rincian kebijakan 2595
Versi kebijakan 2596
Dokumen kebijakan JSON 2596
Pelajari selengkapnya 2597
AWSMigrationHubOrchestratorServiceRolePolicy 2597
Menggunakan kebijakan ini 2597
Rincian kebijakan 2598
Versi kebijakan 2598
Dokumen kebijakan JSON 2598
Pelajari selengkapnya 2601

AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess 2602
Menggunakan kebijakan ini 2602
Rincian kebijakan 2602
Versi kebijakan 2602
Dokumen kebijakan JSON 2602
Pelajari selengkapnya 2608
AWSMigrationHubRefactorSpaces-SSMAutomationPolicy 2608
Menggunakan kebijakan ini 2608
Rincian kebijakan 2609
Versi kebijakan 2609
Dokumen kebijakan JSON 2609
Pelajari selengkapnya 2610
AWSMigrationHubRefactorSpacesFullAccess 2611
Menggunakan kebijakan ini 2611
Rincian kebijakan 2611
Versi kebijakan 2611
Dokumen kebijakan JSON 2611
Pelajari selengkapnya 2618
AWSMigrationHubRefactorSpacesServiceRolePolicy 2618
Menggunakan kebijakan ini 2618
Rincian kebijakan 2618
Versi kebijakan 2618
Dokumen kebijakan JSON 2619
Pelajari selengkapnya 2622
AWSMigrationHubSMSAccess 2623
Menggunakan kebijakan ini 2623
Rincian kebijakan 2623
Versi kebijakan 2623
Dokumen kebijakan JSON 2623
Pelajari selengkapnya 2624
AWSMigrationHubStrategyCollector 2624
Menggunakan kebijakan ini 2625
Rincian kebijakan 2625
Versi kebijakan 2625
Dokumen kebijakan JSON 2625
Pelajari selengkapnya 2627

AWSMigrationHubStrategyConsoleFullAccess 2628
Menggunakan kebijakan ini 2628
Rincian kebijakan 2628
Versi kebijakan 2628
Dokumen kebijakan JSON 2628
Pelajari selengkapnya 2630
AWSMigrationHubStrategyServiceRolePolicy 2630
Menggunakan kebijakan ini 2630
Rincian kebijakan 2630
Versi kebijakan 2631
Dokumen kebijakan JSON 2631
Pelajari selengkapnya 2632
AWSMobileHub_FullAccess 2632
Menggunakan kebijakan ini 2632
Rincian kebijakan 2632
Versi kebijakan 2632
Dokumen kebijakan JSON 2633
Pelajari selengkapnya 2634
AWSMobileHub_ReadOnly 2634
Menggunakan kebijakan ini 2635
Rincian kebijakan 2635
Versi kebijakan 2635
Dokumen kebijakan JSON 2635
Pelajari selengkapnya 2636
AWSMSKReplicatorExecutionRole 2636
Menggunakan kebijakan ini 2637
Rincian kebijakan 2637
Versi kebijakan 2637
Dokumen kebijakan JSON 2637
Pelajari selengkapnya 2638
AWSNetworkFirewallFullAccess 2639
Menggunakan kebijakan ini 2639
Rincian kebijakan 2639
Versi kebijakan 2639
Dokumen kebijakan JSON 2639
Pelajari selengkapnya 2643

AWSNetworkFirewallReadOnlyAccess 2643
Menggunakan kebijakan ini 2644
Rincian kebijakan 2644
Versi kebijakan 2644
Dokumen kebijakan JSON 2644
Pelajari selengkapnya 2645
AWSNetworkFirewallServiceRolePolicy 2645
Menggunakan kebijakan ini 2646
Rincian kebijakan 2646
Versi kebijakan 2646
Dokumen kebijakan JSON 2646
Pelajari selengkapnya 2648
AWSNetworkManagerCloudWANServiceRolePolicy 2648
Menggunakan kebijakan ini 2648
Rincian kebijakan 2648
Versi kebijakan 2648
Dokumen kebijakan JSON 2649
Pelajari selengkapnya 2649
AWSNetworkManagerFullAccess 2649
Menggunakan kebijakan ini 2649
Rincian kebijakan 2649
Versi kebijakan 2650
Dokumen kebijakan JSON 2650
Pelajari selengkapnya 2650
AWSNetworkManagerReadOnlyAccess 2651
Menggunakan kebijakan ini 2651
Rincian kebijakan 2651
Versi kebijakan 2651
Dokumen kebijakan JSON 2651
Pelajari selengkapnya 2652
AWSNetworkManagerServiceRolePolicy 2652
Menggunakan kebijakan ini 2652
Rincian kebijakan 2652
Versi kebijakan 2653
Dokumen kebijakan JSON 2653
Pelajari selengkapnya 2654

AWSObservabilityAdminServiceRolePolicy 2654
Menggunakan kebijakan ini 2654
Rincian kebijakan 2654
Versi kebijakan 2654
Dokumen kebijakan JSON 2655
Pelajari selengkapnya 2657
AWSOpsWorks_FullAccess 2657
Menggunakan kebijakan ini 2657
Rincian kebijakan 2657
Versi kebijakan 2658
Dokumen kebijakan JSON 2658
Pelajari selengkapnya 2659
AWSOpsWorksCloudWatchLogs 2659
Menggunakan kebijakan ini 2659
Rincian kebijakan 2659
Versi kebijakan 2660
Dokumen kebijakan JSON 2660
Pelajari selengkapnya 2660
AWSOpsWorksCMInstanceProfileRole 2660
Menggunakan kebijakan ini 2661
Rincian kebijakan 2661
Versi kebijakan 2661
Dokumen kebijakan JSON 2661
Pelajari selengkapnya 2662
AWSOpsWorksCMServiceRole 2662
Menggunakan kebijakan ini 2662
Rincian kebijakan 2663
Versi kebijakan 2663
Dokumen kebijakan JSON 2663
Pelajari selengkapnya 2667
AWSOpsWorksInstanceRegistration 2667
Menggunakan kebijakan ini 2667
Rincian kebijakan 2668
Versi kebijakan 2668
Dokumen kebijakan JSON 2668
Pelajari selengkapnya 2668

AWSOpsWorksRegisterCLI_EC2 2669
Menggunakan kebijakan ini 2669
Rincian kebijakan 2669
Versi kebijakan 2669
Dokumen kebijakan JSON 2669
Pelajari selengkapnya 2670
AWSOpsWorksRegisterCLI_OnPremises 2670
Menggunakan kebijakan ini 2670
Rincian kebijakan 2671
Versi kebijakan 2671
Dokumen kebijakan JSON 2671
Pelajari selengkapnya 2673
AWSOrganizationsFullAccess 2673
Menggunakan kebijakan ini 2673
Rincian kebijakan 2673
Versi kebijakan 2673
Dokumen kebijakan JSON 2673
Pelajari selengkapnya 2674
AWSOrganizationsReadOnlyAccess 2675
Menggunakan kebijakan ini 2675
Rincian kebijakan 2675
Versi kebijakan 2675
Dokumen kebijakan JSON 2675
Pelajari selengkapnya 2676
AWSOrganizationsServiceTrustPolicy 2676
Menggunakan kebijakan ini 2676
Rincian kebijakan 2676
Versi kebijakan 2677
Dokumen kebijakan JSON 2677
Pelajari selengkapnya 2677
AWSOutpostsAuthorizeServerPolicy 2678
Menggunakan kebijakan ini 2678
Rincian kebijakan 2678
Versi kebijakan 2678
Dokumen kebijakan JSON 2678
Pelajari selengkapnya 2679

AWSOutpostsServiceRolePolicy 2679
Menggunakan kebijakan ini 2679
Rincian kebijakan 2679
Versi kebijakan 2679
Dokumen kebijakan JSON 2680
Pelajari selengkapnya 2681
AWSPanoramaApplianceRolePolicy 2682
Menggunakan kebijakan ini 2682
Rincian kebijakan 2682
Versi kebijakan 2682
Dokumen kebijakan JSON 2682
Pelajari selengkapnya 2683
AWSPanoramaApplianceServiceRolePolicy 2683
Menggunakan kebijakan ini 2683
Rincian kebijakan 2683
Versi kebijakan 2684
Dokumen kebijakan JSON 2684
Pelajari selengkapnya 2685
AWSPanoramaFullAccess 2685
Menggunakan kebijakan ini 2685
Rincian kebijakan 2686
Versi kebijakan 2686
Dokumen kebijakan JSON 2686
Pelajari selengkapnya 2688
AWSPanoramaGreengrassGroupRolePolicy 2689
Menggunakan kebijakan ini 2689
Rincian kebijakan 2689
Versi kebijakan 2689
Dokumen kebijakan JSON 2689
Pelajari selengkapnya 2691
AWSPanoramaSageMakerRolePolicy 2691
Menggunakan kebijakan ini 2691
Rincian kebijakan 2691
Versi kebijakan 2691
Dokumen kebijakan JSON 2692
Pelajari selengkapnya 2692

AWSPanoramaServiceLinkedRolePolicy 2692
Menggunakan kebijakan ini 2693
Rincian kebijakan 2693
Versi kebijakan 2693
Dokumen kebijakan JSON 2693
Pelajari selengkapnya 2696
AWSPanoramaServiceRolePolicy 2696
Menggunakan kebijakan ini 2696
Rincian kebijakan 2696
Versi kebijakan 2696
Dokumen kebijakan JSON 2697
Pelajari selengkapnya 2703
AWSPartnerCentralFullAccess 2704
Menggunakan kebijakan ini 2704
Rincian kebijakan 2704
Versi kebijakan 2704
Dokumen kebijakan JSON 2704
Pelajari selengkapnya 2706
AWSPartnerCentralOpportunityManagement 2706
Menggunakan kebijakan ini 2706
Rincian kebijakan 2706
Versi kebijakan 2706
Dokumen kebijakan JSON 2707
Pelajari selengkapnya 2708
AWSPartnerCentralSandboxFullAccess 2708
Menggunakan kebijakan ini 2709
Rincian kebijakan 2709
Versi kebijakan 2709
Dokumen kebijakan JSON 2709
Pelajari selengkapnya 2710
AWSPartnerCentralSellingResourceSnapshotJobExecutionRolePolicy 2710
Menggunakan kebijakan ini 2710
Rincian kebijakan 2711
Versi kebijakan 2711
Dokumen kebijakan JSON 2711
Pelajari selengkapnya 2712

AWSPartnerLedSupportReadOnlyAccess 2712
Menggunakan kebijakan ini 2712
Rincian kebijakan 2712
Versi kebijakan 2712
Dokumen kebijakan JSON 2713
Pelajari selengkapnya 2750
AWSPCSComputeNodePolicy 2750
Menggunakan kebijakan ini 2750
Rincian kebijakan 2750
Versi kebijakan 2750
Dokumen kebijakan JSON 2750
Pelajari selengkapnya 2751
AWSPCSServiceRolePolicy 2751
Menggunakan kebijakan ini 2751
Rincian kebijakan 2751
Versi kebijakan 2751
Dokumen kebijakan JSON 2752
Pelajari selengkapnya 2757
AWSPriceListServiceFullAccess 2757
Menggunakan kebijakan ini 2757
Rincian kebijakan 2757
Versi kebijakan 2757
Dokumen kebijakan JSON 2757
Pelajari selengkapnya 2758
AWSPrivateCAAuditor 2758
Menggunakan kebijakan ini 2758
Rincian kebijakan 2758
Versi kebijakan 2758
Dokumen kebijakan JSON 2759
Pelajari selengkapnya 2759
AWSPrivateCAConnectorForKubernetesPolicy 2760
Menggunakan kebijakan ini 2760
Rincian kebijakan 2760
Versi kebijakan 2760
Dokumen kebijakan JSON 2760
Pelajari selengkapnya 2761

AWSPrivateCAFullAccess 2761
Menggunakan kebijakan ini 2761
Rincian kebijakan 2761
Versi kebijakan 2761
Dokumen kebijakan JSON 2762
Pelajari selengkapnya 2762
AWSPrivateCAPrivilegedUser 2762
Menggunakan kebijakan ini 2762
Rincian kebijakan 2762
Versi kebijakan 2763
Dokumen kebijakan JSON 2763
Pelajari selengkapnya 2764
AWSPrivateCAReadOnly 2764
Menggunakan kebijakan ini 2764
Rincian kebijakan 2764
Versi kebijakan 2765
Dokumen kebijakan JSON 2765
Pelajari selengkapnya 2765
AWSPrivateCAUser 2766
Menggunakan kebijakan ini 2766
Rincian kebijakan 2766
Versi kebijakan 2766
Dokumen kebijakan JSON 2766
Pelajari selengkapnya 2767
AWSPrivateMarketplaceAdminFullAccess 2768
Menggunakan kebijakan ini 2768
Rincian kebijakan 2768
Versi kebijakan 2768
Dokumen kebijakan JSON 2768
Pelajari selengkapnya 2771
AWSPrivateMarketplaceRequests 2771
Menggunakan kebijakan ini 2771
Rincian kebijakan 2772
Versi kebijakan 2772
Dokumen kebijakan JSON 2772
Pelajari selengkapnya 2772

AWSPrivateNetworksServiceRolePolicy 2773
Menggunakan kebijakan ini 2773
Rincian kebijakan 2773
Versi kebijakan 2773
Dokumen kebijakan JSON 2773
Pelajari selengkapnya 2774
AWSProtonCodeBuildProvisioningBasicAccess 2774
Menggunakan kebijakan ini 2774
Rincian kebijakan 2774
Versi kebijakan 2774
Dokumen kebijakan JSON 2775
Pelajari selengkapnya 2775
AWSProtonCodeBuildProvisioningServiceRolePolicy 2775
Menggunakan kebijakan ini 2776
Rincian kebijakan 2776
Versi kebijakan 2776
Dokumen kebijakan JSON 2776
Pelajari selengkapnya 2777
AWSProtonDeveloperAccess 2778
Menggunakan kebijakan ini 2778
Rincian kebijakan 2778
Versi kebijakan 2778
Dokumen kebijakan JSON 2778
Pelajari selengkapnya 2781
AWSProtonFullAccess 2781
Menggunakan kebijakan ini 2781
Rincian kebijakan 2781
Versi kebijakan 2781
Dokumen kebijakan JSON 2781
Pelajari selengkapnya 2784
AWSProtonReadOnlyAccess 2784
Menggunakan kebijakan ini 2784
Rincian kebijakan 2784
Versi kebijakan 2784
Dokumen kebijakan JSON 2784
Pelajari selengkapnya 2786

AWSProtonServiceGitSyncServiceRolePolicy 2786
Menggunakan kebijakan ini 2786
Rincian kebijakan 2786
Versi kebijakan 2787
Dokumen kebijakan JSON 2787
Pelajari selengkapnya 2787
AWSProtonSyncServiceRolePolicy 2788
Menggunakan kebijakan ini 2788
Rincian kebijakan 2788
Versi kebijakan 2788
Dokumen kebijakan JSON 2788
Pelajari selengkapnya 2789
AWSPurchaseOrdersServiceRolePolicy 2790
Menggunakan kebijakan ini 2790
Rincian kebijakan 2790
Versi kebijakan 2790
Dokumen kebijakan JSON 2790
Pelajari selengkapnya 2791
AWSQuickSetupCFGCPacksPermissionsBoundary 2791
Menggunakan kebijakan ini 2792
Rincian kebijakan 2792
Versi kebijakan 2792
Dokumen kebijakan JSON 2792
Pelajari selengkapnya 2795
AWSQuickSetupDeploymentRolePolicy 2795
Menggunakan kebijakan ini 2795
Rincian kebijakan 2795
Versi kebijakan 2796
Dokumen kebijakan JSON 2796
Pelajari selengkapnya 2804
AWSQuickSetupDevOpsGuruPermissionsBoundary 2804
Menggunakan kebijakan ini 2804
Rincian kebijakan 2804
Versi kebijakan 2804
Dokumen kebijakan JSON 2805
Pelajari selengkapnya 2807

AWSQuickSetupDistributorPermissionsBoundary 2808
Menggunakan kebijakan ini 2808
Rincian kebijakan 2808
Versi kebijakan 2808
Dokumen kebijakan JSON 2808
Pelajari selengkapnya 2814
AWSQuickSetupEnableAREXExecutionPolicy 2814
Menggunakan kebijakan ini 2814
Rincian kebijakan 2814
Versi kebijakan 2815
Dokumen kebijakan JSON 2815
Pelajari selengkapnya 2816
AWSQuickSetupEnableDHMCExecutionPolicy 2817
Menggunakan kebijakan ini 2817
Rincian kebijakan 2817
Versi kebijakan 2817
Dokumen kebijakan JSON 2817
Pelajari selengkapnya 2818
AWSQuickSetupJITNADeploymentRolePolicy 2819
Menggunakan kebijakan ini 2819
Rincian kebijakan 2819
Versi kebijakan 2819
Dokumen kebijakan JSON 2819
Pelajari selengkapnya 2823
AWSQuickSetupManagedInstanceProfileExecutionPolicy 2823
Menggunakan kebijakan ini 2823
Rincian kebijakan 2823
Versi kebijakan 2824
Dokumen kebijakan JSON 2824
Pelajari selengkapnya 2828
AWSQuickSetupManageJITNAResourcesExecutionPolicy 2828
Menggunakan kebijakan ini 2828
Rincian kebijakan 2828
Versi kebijakan 2829
Dokumen kebijakan JSON 2829
Pelajari selengkapnya 2831

AWSQuickSetupPatchPolicyBaselineAccess 2831
Menggunakan kebijakan ini 2831
Rincian kebijakan 2831
Versi kebijakan 2832
Dokumen kebijakan JSON 2832
Pelajari selengkapnya 2833
AWSQuickSetupPatchPolicyDeploymentRolePolicy 2833
Menggunakan kebijakan ini 2833
Rincian kebijakan 2833
Versi kebijakan 2833
Dokumen kebijakan JSON 2833
Pelajari selengkapnya 2841
AWSQuickSetupPatchPolicyPermissionsBoundary 2842
Menggunakan kebijakan ini 2842
Rincian kebijakan 2842
Versi kebijakan 2842
Dokumen kebijakan JSON 2842
Pelajari selengkapnya 2850
AWSQuickSetupSchedulerPermissionsBoundary 2851
Menggunakan kebijakan ini 2851
Rincian kebijakan 2851
Versi kebijakan 2851
Dokumen kebijakan JSON 2851
Pelajari selengkapnya 2854
AWSQuickSetupSSMDeploymentRolePolicy 2855
Menggunakan kebijakan ini 2855
Rincian kebijakan 2855
Versi kebijakan 2855
Dokumen kebijakan JSON 2855
Pelajari selengkapnya 2864
AWSQuickSetupSSMDeploymentS3BucketRolePolicy 2864
Menggunakan kebijakan ini 2864
Rincian kebijakan 2864
Versi kebijakan 2864
Dokumen kebijakan JSON 2865
Pelajari selengkapnya 2865

AWSQuickSetupSSMHostMgmtPermissionsBoundary 2866
Menggunakan kebijakan ini 2866
Rincian kebijakan 2866
Versi kebijakan 2866
Dokumen kebijakan JSON 2866
Pelajari selengkapnya 2872
AWSQuickSetupSSMLifecycleManagementExecutionPolicy 2872
Menggunakan kebijakan ini 2873
Rincian kebijakan 2873
Versi kebijakan 2873
Dokumen kebijakan JSON 2873
Pelajari selengkapnya 2874
AWSQuickSetupSSMManageResourcesExecutionPolicy 2875
Menggunakan kebijakan ini 2875
Rincian kebijakan 2875
Versi kebijakan 2875
Dokumen kebijakan JSON 2875
Pelajari selengkapnya 2878
AWSQuickSightAssetBundleExportPolicy 2878
Menggunakan kebijakan ini 2878
Rincian kebijakan 2878
Versi kebijakan 2879
Dokumen kebijakan JSON 2879
Pelajari selengkapnya 2881
AWSQuickSightAssetBundleImportPolicy 2881
Menggunakan kebijakan ini 2881
Rincian kebijakan 2881
Versi kebijakan 2882
Dokumen kebijakan JSON 2882
Pelajari selengkapnya 2885
AWSQuicksightAthenaAccess 2885
Menggunakan kebijakan ini 2885
Rincian kebijakan 2885
Versi kebijakan 2885
Dokumen kebijakan JSON 2886
Pelajari selengkapnya 2888

AWSQuickSightDescribeRDS 2888
Menggunakan kebijakan ini 2888
Rincian kebijakan 2888
Versi kebijakan 2888
Dokumen kebijakan JSON 2889
Pelajari selengkapnya 2889
AWSQuickSightDescribeRedshift 2889
Menggunakan kebijakan ini 2889
Rincian kebijakan 2890
Versi kebijakan 2890
Dokumen kebijakan JSON 2890
Pelajari selengkapnya 2890
AWSQuickSightElasticsearchPolicy 2891
Menggunakan kebijakan ini 2891
Rincian kebijakan 2891
Versi kebijakan 2891
Dokumen kebijakan JSON 2891
Pelajari selengkapnya 2892
AWSQuickSightIoTAnalyticsAccess 2893
Menggunakan kebijakan ini 2893
Rincian kebijakan 2893
Versi kebijakan 2893
Dokumen kebijakan JSON 2893
Pelajari selengkapnya 2894
AWSQuickSightListIAM 2894
Menggunakan kebijakan ini 2894
Rincian kebijakan 2894
Versi kebijakan 2894
Dokumen kebijakan JSON 2895
Pelajari selengkapnya 2895
AWSQuicksightOpenSearchPolicy 2895
Menggunakan kebijakan ini 2895
Rincian kebijakan 2895
Versi kebijakan 2896
Dokumen kebijakan JSON 2896
Pelajari selengkapnya 2897

AWSQuickSightSageMakerPolicy 2897
Menggunakan kebijakan ini 2897
Rincian kebijakan 2897
Versi kebijakan 2898
Dokumen kebijakan JSON 2898
Pelajari selengkapnya 2899
AWSQuickSightSecretsManagerWriteAccess 2899
Menggunakan kebijakan ini 2899
Rincian kebijakan 2899
Versi kebijakan 2900
Dokumen kebijakan JSON 2900
Pelajari selengkapnya 2901
AWSQuickSightSecretsManagerWritePolicy 2901
Menggunakan kebijakan ini 2901
Rincian kebijakan 2901
Versi kebijakan 2901
Dokumen kebijakan JSON 2902
Pelajari selengkapnya 2903
AWSQuickSightTimestreamPolicy 2903
Menggunakan kebijakan ini 2903
Rincian kebijakan 2903
Versi kebijakan 2903
Dokumen kebijakan JSON 2903
Pelajari selengkapnya 2904
AWSReachabilityAnalyzerServiceRolePolicy 2904
Menggunakan kebijakan ini 2904
Rincian kebijakan 2905
Versi kebijakan 2905
Dokumen kebijakan JSON 2905
Pelajari selengkapnya 2907
AWSRefactoringToolkitFullAccess 2907
Menggunakan kebijakan ini 2908
Rincian kebijakan 2908
Versi kebijakan 2908
Dokumen kebijakan JSON 2908
Pelajari selengkapnya 2922

AWSRefactoringToolkitSidecarPolicy 2922
Menggunakan kebijakan ini 2922
Rincian kebijakan 2922
Versi kebijakan 2922
Dokumen kebijakan JSON 2923
Pelajari selengkapnya 2924
AWSrePostPrivateCloudWatchAccess 2924
Menggunakan kebijakan ini 2924
Rincian kebijakan 2924
Versi kebijakan 2924
Dokumen kebijakan JSON 2925
Pelajari selengkapnya 2925
AWSRepostSpaceSupportOperationsPolicy 2925
Menggunakan kebijakan ini 2925
Rincian kebijakan 2926
Versi kebijakan 2926
Dokumen kebijakan JSON 2926
Pelajari selengkapnya 2926
AWSResilienceHubAsssessmentExecutionPolicy 2927
Menggunakan kebijakan ini 2927
Rincian kebijakan 2927
Versi kebijakan 2927
Dokumen kebijakan JSON 2927
Pelajari selengkapnya 2932
AWSResourceAccessManagerFullAccess 2932
Menggunakan kebijakan ini 2932
Rincian kebijakan 2933
Versi kebijakan 2933
Dokumen kebijakan JSON 2933
Pelajari selengkapnya 2933
AWSResourceAccessManagerReadOnlyAccess 2934
Menggunakan kebijakan ini 2934
Rincian kebijakan 2934
Versi kebijakan 2934
Dokumen kebijakan JSON 2934
Pelajari selengkapnya 2935

AWSResourceAccessManagerResourceShareParticipantAccess 2935
Menggunakan kebijakan ini 2935
Rincian kebijakan 2935
Versi kebijakan 2935
Dokumen kebijakan JSON 2936
Pelajari selengkapnya 2936
AWSResourceAccessManagerServiceRolePolicy 2936
Menggunakan kebijakan ini 2937
Rincian kebijakan 2937
Versi kebijakan 2937
Dokumen kebijakan JSON 2937
Pelajari selengkapnya 2938
AWSResourceExplorerFullAccess 2938
Menggunakan kebijakan ini 2938
Rincian kebijakan 2938
Versi kebijakan 2939
Dokumen kebijakan JSON 2939
Pelajari selengkapnya 2940
AWSResourceExplorerOrganizationsAccess 2940
Menggunakan kebijakan ini 2940
Rincian kebijakan 2940
Versi kebijakan 2940
Dokumen kebijakan JSON 2941
Pelajari selengkapnya 2942
AWSResourceExplorerReadOnlyAccess 2942
Menggunakan kebijakan ini 2943
Rincian kebijakan 2943
Versi kebijakan 2943
Dokumen kebijakan JSON 2943
Pelajari selengkapnya 2944
AWSResourceExplorerServiceRolePolicy 2944
Menggunakan kebijakan ini 2944
Rincian kebijakan 2944
Versi kebijakan 2944
Dokumen kebijakan JSON 2945
Pelajari selengkapnya 2961

AWSResourceGroupsReadOnlyAccess 2961
Menggunakan kebijakan ini 2961
Rincian kebijakan 2961
Versi kebijakan 2961
Dokumen kebijakan JSON 2961
Pelajari selengkapnya 2963
AWSRoboMaker_FullAccess 2963
Menggunakan kebijakan ini 2963
Rincian kebijakan 2963
Versi kebijakan 2963
Dokumen kebijakan JSON 2964
Pelajari selengkapnya 2965
AWSRoboMakerReadOnlyAccess 2965
Menggunakan kebijakan ini 2965
Rincian kebijakan 2965
Versi kebijakan 2966
Dokumen kebijakan JSON 2966
Pelajari selengkapnya 2966
AWSRoboMakerServicePolicy 2966
Menggunakan kebijakan ini 2967
Rincian kebijakan 2967
Versi kebijakan 2967
Dokumen kebijakan JSON 2967
Pelajari selengkapnya 2969
AWSRoboMakerServiceRolePolicy 2969
Menggunakan kebijakan ini 2969
Rincian kebijakan 2969
Versi kebijakan 2969
Dokumen kebijakan JSON 2970
Pelajari selengkapnya 2971
AWSRolesAnywhereServicePolicy 2971
Menggunakan kebijakan ini 2971
Rincian kebijakan 2971
Versi kebijakan 2972
Dokumen kebijakan JSON 2972
Pelajari selengkapnya 2972

AWSS3OnOutpostsServiceRolePolicy 2973
Menggunakan kebijakan ini 2973
Rincian kebijakan 2973
Versi kebijakan 2973
Dokumen kebijakan JSON 2973
Pelajari selengkapnya 2976
AWSSavingsPlansFullAccess 2976
Menggunakan kebijakan ini 2976
Rincian kebijakan 2976
Versi kebijakan 2977
Dokumen kebijakan JSON 2977
Pelajari selengkapnya 2977
AWSSavingsPlansReadOnlyAccess 2977
Menggunakan kebijakan ini 2977
Rincian kebijakan 2978
Versi kebijakan 2978
Dokumen kebijakan JSON 2978
Pelajari selengkapnya 2978
AWSSecurityHubFullAccess 2979
Menggunakan kebijakan ini 2979
Rincian kebijakan 2979
Versi kebijakan 2979
Dokumen kebijakan JSON 2979
Pelajari selengkapnya 2980
AWSSecurityHubOrganizationsAccess 2980
Menggunakan kebijakan ini 2981
Rincian kebijakan 2981
Versi kebijakan 2981
Dokumen kebijakan JSON 2981
Pelajari selengkapnya 2983
AWSSecurityHubReadOnlyAccess 2983
Menggunakan kebijakan ini 2984
Rincian kebijakan 2984
Versi kebijakan 2984
Dokumen kebijakan JSON 2984
Pelajari selengkapnya 2985

AWSSecurityHubServiceRolePolicy 2985
Menggunakan kebijakan ini 2985
Rincian kebijakan 2985
Versi kebijakan 2985
Dokumen kebijakan JSON 2986
Pelajari selengkapnya 2988
AWSSecurityHubV2ServiceRolePolicy 2988
Menggunakan kebijakan ini 2988
Rincian kebijakan 2988
Versi kebijakan 2988
Dokumen kebijakan JSON 2988
Pelajari selengkapnya 2991
AWSSecurityIncidentResponseCaseFullAccess 2991
Menggunakan kebijakan ini 2991
Rincian kebijakan 2991
Versi kebijakan 2991
Dokumen kebijakan JSON 2991
Pelajari selengkapnya 2993
AWSSecurityIncidentResponseFullAccess 2993
Menggunakan kebijakan ini 2993
Rincian kebijakan 2993
Versi kebijakan 2994
Dokumen kebijakan JSON 2994
Pelajari selengkapnya 2996
AWSSecurityIncidentResponseReadOnlyAccess 2996
Menggunakan kebijakan ini 2996
Rincian kebijakan 2996
Versi kebijakan 2997
Dokumen kebijakan JSON 2997
Pelajari selengkapnya 2997
AWSSecurityIncidentResponseServiceRolePolicy 2998
Menggunakan kebijakan ini 2998
Rincian kebijakan 2998
Versi kebijakan 2998
Dokumen kebijakan JSON 2998
Pelajari selengkapnya 2999

AWSSecurityIncidentResponseTriageServiceRolePolicy 2999
Menggunakan kebijakan ini 3000
Rincian kebijakan 3000
Versi kebijakan 3000
Dokumen kebijakan JSON 3000
Pelajari selengkapnya 3002
AWSServiceCatalogAdminFullAccess 3003
Menggunakan kebijakan ini 3003
Rincian kebijakan 3003
Versi kebijakan 3003
Dokumen kebijakan JSON 3003
Pelajari selengkapnya 3006
AWSServiceCatalogAdminReadOnlyAccess 3006
Menggunakan kebijakan ini 3006
Rincian kebijakan 3006
Versi kebijakan 3007
Dokumen kebijakan JSON 3007
Pelajari selengkapnya 3008
AWSServiceCatalogAppRegistryFullAccess 3008
Menggunakan kebijakan ini 3008
Rincian kebijakan 3008
Versi kebijakan 3009
Dokumen kebijakan JSON 3009
Pelajari selengkapnya 3011
AWSServiceCatalogAppRegistryReadOnlyAccess 3011
Menggunakan kebijakan ini 3011
Rincian kebijakan 3012
Versi kebijakan 3012
Dokumen kebijakan JSON 3012
Pelajari selengkapnya 3013
AWSServiceCatalogAppRegistryServiceRolePolicy 3013
Menggunakan kebijakan ini 3013
Rincian kebijakan 3013
Versi kebijakan 3013
Dokumen kebijakan JSON 3014
Pelajari selengkapnya 3015

AWSServiceCatalogEndUserFullAccess 3015
Menggunakan kebijakan ini 3015
Rincian kebijakan 3015
Versi kebijakan 3015
Dokumen kebijakan JSON 3016
Pelajari selengkapnya 3018
AWSServiceCatalogEndUserReadOnlyAccess 3018
Menggunakan kebijakan ini 3018
Rincian kebijakan 3018
Versi kebijakan 3018
Dokumen kebijakan JSON 3019
Pelajari selengkapnya 3020
AWSServiceCatalogOrgsDataSyncServiceRolePolicy 3020
Menggunakan kebijakan ini 3021
Rincian kebijakan 3021
Versi kebijakan 3021
Dokumen kebijakan JSON 3021
Pelajari selengkapnya 3022
AWSServiceCatalogSyncServiceRolePolicy 3022
Menggunakan kebijakan ini 3022
Rincian kebijakan 3022
Versi kebijakan 3022
Dokumen kebijakan JSON 3023
Pelajari selengkapnya 3024
AWSServiceRoleForAmazonEKSNodegroup 3024
Menggunakan kebijakan ini 3024
Rincian kebijakan 3024
Versi kebijakan 3024
Dokumen kebijakan JSON 3025
Pelajari selengkapnya 3030
AWSServiceRoleForAmazonQDeveloper 3030
Menggunakan kebijakan ini 3030
Rincian kebijakan 3030
Versi kebijakan 3031
Dokumen kebijakan JSON 3031
Pelajari selengkapnya 3031

AWSServiceRoleForAWSTransform 3032
Menggunakan kebijakan ini 3032
Rincian kebijakan 3032
Versi kebijakan 3032
Dokumen kebijakan JSON 3032
Pelajari selengkapnya 3033
AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy 3033
Menggunakan kebijakan ini 3033
Rincian kebijakan 3033
Versi kebijakan 3034
Dokumen kebijakan JSON 3034
Pelajari selengkapnya 3034
AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy 3034
Menggunakan kebijakan ini 3035
Rincian kebijakan 3035
Versi kebijakan 3035
Dokumen kebijakan JSON 3035
Pelajari selengkapnya 3036
AWSServiceRoleForCodeGuru-Profiler 3036
Menggunakan kebijakan ini 3036
Rincian kebijakan 3036
Versi kebijakan 3036
Dokumen kebijakan JSON 3037
Pelajari selengkapnya 3037
AWSServiceRoleForCodeWhispererPolicy 3037
Menggunakan kebijakan ini 3037
Rincian kebijakan 3037
Versi kebijakan 3038
Dokumen kebijakan JSON 3038
Pelajari selengkapnya 3040
AWSServiceRoleForEC2ScheduledInstances 3040
Menggunakan kebijakan ini 3040
Rincian kebijakan 3040
Versi kebijakan 3040
Dokumen kebijakan JSON 3040
Pelajari selengkapnya 3041

AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy 3042
Menggunakan kebijakan ini 3042
Rincian kebijakan 3042
Versi kebijakan 3042
Dokumen kebijakan JSON 3042
Pelajari selengkapnya 3043
AWSServiceRoleForImageBuilder 3043
Menggunakan kebijakan ini 3043
Rincian kebijakan 3043
Versi kebijakan 3043
Dokumen kebijakan JSON 3044
Pelajari selengkapnya 3054
AWSServiceRoleForIoTSiteWise 3054
Menggunakan kebijakan ini 3054
Rincian kebijakan 3054
Versi kebijakan 3054
Dokumen kebijakan JSON 3055
Pelajari selengkapnya 3056
AWSServiceRoleForLogDeliveryPolicy 3056
Menggunakan kebijakan ini 3056
Rincian kebijakan 3056
Versi kebijakan 3057
Dokumen kebijakan JSON 3057
Pelajari selengkapnya 3057
AWSServiceRoleForMonitronPolicy 3058
Menggunakan kebijakan ini 3058
Rincian kebijakan 3058
Versi kebijakan 3058
Dokumen kebijakan JSON 3058
Pelajari selengkapnya 3059
AWSServiceRoleForNeptuneGraphPolicy 3059
Menggunakan kebijakan ini 3059
Rincian kebijakan 3059
Versi kebijakan 3060
Dokumen kebijakan JSON 3060
Pelajari selengkapnya 3061

AWSServiceRoleForPrivateMarketplaceAdminPolicy 3061
Menggunakan kebijakan ini 3061
Rincian kebijakan 3062
Versi kebijakan 3062
Dokumen kebijakan JSON 3062
Pelajari selengkapnya 3064
AWSServiceRoleForProcurementInsightsPolicy 3064
Menggunakan kebijakan ini 3064
Rincian kebijakan 3064
Versi kebijakan 3064
Dokumen kebijakan JSON 3064
Pelajari selengkapnya 3065
AWSServiceRoleForSMS 3065
Menggunakan kebijakan ini 3065
Rincian kebijakan 3065
Versi kebijakan 3066
Dokumen kebijakan JSON 3066
Pelajari selengkapnya 3072
AWSServiceRoleForUserSubscriptions 3073
Menggunakan kebijakan ini 3073
Rincian kebijakan 3073
Versi kebijakan 3073
Dokumen kebijakan JSON 3073
Pelajari selengkapnya 3074
AWSServiceRolePolicyForBackupReports 3074
Menggunakan kebijakan ini 3074
Rincian kebijakan 3074
Versi kebijakan 3075
Dokumen kebijakan JSON 3075
Pelajari selengkapnya 3076
AWSServiceRolePolicyForBackupRestoreTesting 3076
Menggunakan kebijakan ini 3076
Rincian kebijakan 3077
Versi kebijakan 3077
Dokumen kebijakan JSON 3077
Pelajari selengkapnya 3080

AWSServiceRolePolicyForWorkspacesInstances 3080
Menggunakan kebijakan ini 3080
Rincian kebijakan 3080
Versi kebijakan 3080
Dokumen kebijakan JSON 3081
Pelajari selengkapnya 3081
AWSShieldDRTAccessPolicy 3082
Menggunakan kebijakan ini 3082
Rincian kebijakan 3082
Versi kebijakan 3082
Dokumen kebijakan JSON 3082
Pelajari selengkapnya 3083
AWSShieldServiceRolePolicy 3083
Menggunakan kebijakan ini 3084
Rincian kebijakan 3084
Versi kebijakan 3084
Dokumen kebijakan JSON 3084
Pelajari selengkapnya 3085
AWSSocialMessagingServiceRolePolicy 3085
Menggunakan kebijakan ini 3085
Rincian kebijakan 3085
Versi kebijakan 3085
Dokumen kebijakan JSON 3086
Pelajari selengkapnya 3086
AWSSSMForSAPServiceLinkedRolePolicy 3086
Menggunakan kebijakan ini 3086
Rincian kebijakan 3086
Versi kebijakan 3087
Dokumen kebijakan JSON 3087
Pelajari selengkapnya 3095
AWSSSMOpsInsightsServiceRolePolicy 3095
Menggunakan kebijakan ini 3096
Rincian kebijakan 3096
Versi kebijakan 3096
Dokumen kebijakan JSON 3096
Pelajari selengkapnya 3097

AWSSSODirectoryAdministrator 3097
Menggunakan kebijakan ini 3097
Rincian kebijakan 3097
Versi kebijakan 3098
Dokumen kebijakan JSON 3098
Pelajari selengkapnya 3098
AWSSSODirectoryReadOnly 3098
Menggunakan kebijakan ini 3099
Rincian kebijakan 3099
Versi kebijakan 3099
Dokumen kebijakan JSON 3099
Pelajari selengkapnya 3100
AWSSSOMasterAccountAdministrator 3100
Menggunakan kebijakan ini 3100
Rincian kebijakan 3100
Versi kebijakan 3100
Dokumen kebijakan JSON 3101
Pelajari selengkapnya 3103
AWSSSOMemberAccountAdministrator 3103
Menggunakan kebijakan ini 3103
Rincian kebijakan 3103
Versi kebijakan 3103
Dokumen kebijakan JSON 3103
Pelajari selengkapnya 3105
AWSSSOReadOnly 3105
Menggunakan kebijakan ini 3105
Rincian kebijakan 3105
Versi kebijakan 3105
Dokumen kebijakan JSON 3106
Pelajari selengkapnya 3106
AWSSSOServiceRolePolicy 3107
Menggunakan kebijakan ini 3107
Rincian kebijakan 3107
Versi kebijakan 3107
Dokumen kebijakan JSON 3107
Pelajari selengkapnya 3111

AWSStepFunctionsConsoleFullAccess 3111
Menggunakan kebijakan ini 3111
Rincian kebijakan 3111
Versi kebijakan 3112
Dokumen kebijakan JSON 3112
Pelajari selengkapnya 3112
AWSStepFunctionsFullAccess 3113
Menggunakan kebijakan ini 3113
Rincian kebijakan 3113
Versi kebijakan 3113
Dokumen kebijakan JSON 3113
Pelajari selengkapnya 3114
AWSStepFunctionsReadOnlyAccess 3114
Menggunakan kebijakan ini 3114
Rincian kebijakan 3114
Versi kebijakan 3114
Dokumen kebijakan JSON 3115
Pelajari selengkapnya 3115
AWSStorageGatewayFullAccess 3116
Menggunakan kebijakan ini 3116
Rincian kebijakan 3116
Versi kebijakan 3116
Dokumen kebijakan JSON 3116
Pelajari selengkapnya 3117
AWSStorageGatewayReadOnlyAccess 3117
Menggunakan kebijakan ini 3117
Rincian kebijakan 3117
Versi kebijakan 3118
Dokumen kebijakan JSON 3118
Pelajari selengkapnya 3118
AWSStorageGatewayServiceRolePolicy 3119
Menggunakan kebijakan ini 3119
Rincian kebijakan 3119
Versi kebijakan 3119
Dokumen kebijakan JSON 3119
Pelajari selengkapnya 3120

AWSSupplyChainFederationAdminAccess 3120
Menggunakan kebijakan ini 3120
Rincian kebijakan 3120
Versi kebijakan 3121
Dokumen kebijakan JSON 3121
Pelajari selengkapnya 3126
AWSSupportAccess 3126
Menggunakan kebijakan ini 3126
Rincian kebijakan 3127
Versi kebijakan 3127
Dokumen kebijakan JSON 3127
Pelajari selengkapnya 3127
AWSSupportAppFullAccess 3128
Menggunakan kebijakan ini 3128
Rincian kebijakan 3128
Versi kebijakan 3128
Dokumen kebijakan JSON 3128
Pelajari selengkapnya 3129
AWSSupportAppReadOnlyAccess 3129
Menggunakan kebijakan ini 3129
Rincian kebijakan 3130
Versi kebijakan 3130
Dokumen kebijakan JSON 3130
Pelajari selengkapnya 3130
AWSSupportPlansFullAccess 3131
Menggunakan kebijakan ini 3131
Rincian kebijakan 3131
Versi kebijakan 3131
Dokumen kebijakan JSON 3131
Pelajari selengkapnya 3132
AWSSupportPlansReadOnlyAccess 3132
Menggunakan kebijakan ini 3132
Rincian kebijakan 3132
Versi kebijakan 3132
Dokumen kebijakan JSON 3133
Pelajari selengkapnya 3133

AWSSupportServiceRolePolicy 3133
Menggunakan kebijakan ini 3133
Rincian kebijakan 3134
Versi kebijakan 3134
Dokumen kebijakan JSON 3134
Pelajari selengkapnya 3220
AWSSystemsManagerAccountDiscoveryServicePolicy 3221
Menggunakan kebijakan ini 3221
Rincian kebijakan 3221
Versi kebijakan 3221
Dokumen kebijakan JSON 3221
Pelajari selengkapnya 3222
AWSSystemsManagerChangeManagementServicePolicy 3222
Menggunakan kebijakan ini 3222
Rincian kebijakan 3222
Versi kebijakan 3223
Dokumen kebijakan JSON 3223
Pelajari selengkapnya 3224
AWSSystemsManagerEnableConfigRecordingExecutionPolicy 3225
Menggunakan kebijakan ini 3225
Rincian kebijakan 3225
Versi kebijakan 3225
Dokumen kebijakan JSON 3225
Pelajari selengkapnya 3227
AWSSystemsManagerEnableExplorerExecutionPolicy 3228
Menggunakan kebijakan ini 3228
Rincian kebijakan 3228
Versi kebijakan 3228
Dokumen kebijakan JSON 3228
Pelajari selengkapnya 3230
AWSSystemsManagerForSAPFullAccess 3230
Menggunakan kebijakan ini 3230
Rincian kebijakan 3230
Versi kebijakan 3230
Dokumen kebijakan JSON 3230
Pelajari selengkapnya 3232

AWSSystemsManagerForSAPReadOnlyAccess 3232
Menggunakan kebijakan ini 3232
Rincian kebijakan 3232
Versi kebijakan 3232
Dokumen kebijakan JSON 3232
Pelajari selengkapnya 3233
AWSSystemsManagerJustInTimeAccessServicePolicy 3233
Menggunakan kebijakan ini 3233
Rincian kebijakan 3233
Versi kebijakan 3234
Dokumen kebijakan JSON 3234
Pelajari selengkapnya 3238
AWSSystemsManagerJustInTimeAccessTokenPolicy 3238
Menggunakan kebijakan ini 3238
Rincian kebijakan 3238
Versi kebijakan 3239
Dokumen kebijakan JSON 3239
Pelajari selengkapnya 3242
AWSSystemsManagerJustInTimeAccessTokenSessionPolicy 3242
Menggunakan kebijakan ini 3242
Rincian kebijakan 3242
Versi kebijakan 3242
Dokumen kebijakan JSON 3243
Pelajari selengkapnya 3245
AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy 3245
Menggunakan kebijakan ini 3245
Rincian kebijakan 3246
Versi kebijakan 3246
Dokumen kebijakan JSON 3246
Pelajari selengkapnya 3250
AWSSystemsManagerNotificationsServicePolicy 3250
Menggunakan kebijakan ini 3251
Rincian kebijakan 3251
Versi kebijakan 3251
Dokumen kebijakan JSON 3251
Pelajari selengkapnya 3252

AWSSystemsManagerOpsDataSyncServiceRolePolicy 3253
Menggunakan kebijakan ini 3253
Rincian kebijakan 3253
Versi kebijakan 3253
Dokumen kebijakan JSON 3253
Pelajari selengkapnya 3257
AWSThinkboxAssetServerPolicy 3257
Menggunakan kebijakan ini 3257
Rincian kebijakan 3257
Versi kebijakan 3257
Dokumen kebijakan JSON 3258
Pelajari selengkapnya 3258
AWSThinkboxAWSPortalAdminPolicy 3259
Menggunakan kebijakan ini 3259
Rincian kebijakan 3259
Versi kebijakan 3259
Dokumen kebijakan JSON 3259
Pelajari selengkapnya 3269
AWSThinkboxAWSPortalGatewayPolicy 3269
Menggunakan kebijakan ini 3269
Rincian kebijakan 3270
Versi kebijakan 3270
Dokumen kebijakan JSON 3270
Pelajari selengkapnya 3272
AWSThinkboxAWSPortalWorkerPolicy 3272
Menggunakan kebijakan ini 3272
Rincian kebijakan 3272
Versi kebijakan 3272
Dokumen kebijakan JSON 3273
Pelajari selengkapnya 3275
AWSThinkboxDeadlineResourceTrackerAccessPolicy 3275
Menggunakan kebijakan ini 3275
Rincian kebijakan 3275
Versi kebijakan 3275
Dokumen kebijakan JSON 3276
Pelajari selengkapnya 3278

AWSThinkboxDeadlineResourceTrackerAdminPolicy 3278
Menggunakan kebijakan ini 3279
Rincian kebijakan 3279
Versi kebijakan 3279
Dokumen kebijakan JSON 3279
Pelajari selengkapnya 3285
AWSThinkboxDeadlineSpotEventPluginAdminPolicy 3285
Menggunakan kebijakan ini 3285
Rincian kebijakan 3286
Versi kebijakan 3286
Dokumen kebijakan JSON 3286
Pelajari selengkapnya 3289
AWSThinkboxDeadlineSpotEventPluginWorkerPolicy 3289
Menggunakan kebijakan ini 3289
Rincian kebijakan 3289
Versi kebijakan 3289
Dokumen kebijakan JSON 3290
Pelajari selengkapnya 3291
AWSTransferConsoleFullAccess 3291
Menggunakan kebijakan ini 3291
Rincian kebijakan 3291
Versi kebijakan 3292
Dokumen kebijakan JSON 3292
Pelajari selengkapnya 3293
AWSTransferFullAccess 3293
Menggunakan kebijakan ini 3293
Rincian kebijakan 3293
Versi kebijakan 3293
Dokumen kebijakan JSON 3294
Pelajari selengkapnya 3294
AWSTransferLoggingAccess 3295
Menggunakan kebijakan ini 3295
Rincian kebijakan 3295
Versi kebijakan 3295
Dokumen kebijakan JSON 3295
Pelajari selengkapnya 3296

AWSTransferReadOnlyAccess 3296
Menggunakan kebijakan ini 3296
Rincian kebijakan 3296
Versi kebijakan 3296
Dokumen kebijakan JSON 3297
Pelajari selengkapnya 3297
AWSTrustedAdvisorPriorityFullAccess 3297
Menggunakan kebijakan ini 3298
Rincian kebijakan 3298
Versi kebijakan 3298
Dokumen kebijakan JSON 3298
Pelajari selengkapnya 3300
AWSTrustedAdvisorPriorityReadOnlyAccess 3300
Menggunakan kebijakan ini 3300
Rincian kebijakan 3300
Versi kebijakan 3301
Dokumen kebijakan JSON 3301
Pelajari selengkapnya 3302
AWSTrustedAdvisorReportingServiceRolePolicy 3302
Menggunakan kebijakan ini 3302
Rincian kebijakan 3302
Versi kebijakan 3302
Dokumen kebijakan JSON 3303
Pelajari selengkapnya 3303
AWSTrustedAdvisorServiceRolePolicy 3303
Menggunakan kebijakan ini 3304
Rincian kebijakan 3304
Versi kebijakan 3304
Dokumen kebijakan JSON 3304
Pelajari selengkapnya 3307
AWSUserNotificationsServiceLinkedRolePolicy 3307
Menggunakan kebijakan ini 3307
Rincian kebijakan 3307
Versi kebijakan 3308
Dokumen kebijakan JSON 3308
Pelajari selengkapnya 3309

AWSVendorInsightsAssessorFullAccess 3309
Menggunakan kebijakan ini 3309
Rincian kebijakan 3309
Versi kebijakan 3310
Dokumen kebijakan JSON 3310
Pelajari selengkapnya 3311
AWSVendorInsightsAssessorReadOnly 3311
Menggunakan kebijakan ini 3311
Rincian kebijakan 3311
Versi kebijakan 3312
Dokumen kebijakan JSON 3312
Pelajari selengkapnya 3312
AWSVendorInsightsVendorFullAccess 3313
Menggunakan kebijakan ini 3313
Rincian kebijakan 3313
Versi kebijakan 3313
Dokumen kebijakan JSON 3313
Pelajari selengkapnya 3315
AWSVendorInsightsVendorReadOnly 3315
Menggunakan kebijakan ini 3315
Rincian kebijakan 3315
Versi kebijakan 3316
Dokumen kebijakan JSON 3316
Pelajari selengkapnya 3317
AWSVpcLatticeServiceRolePolicy 3317
Menggunakan kebijakan ini 3317
Rincian kebijakan 3317
Versi kebijakan 3317
Dokumen kebijakan JSON 3318
Pelajari selengkapnya 3320
AWSVPCS2SVpnServiceRolePolicy 3320
Menggunakan kebijakan ini 3321
Rincian kebijakan 3321
Versi kebijakan 3321
Dokumen kebijakan JSON 3321
Pelajari selengkapnya 3322

AWSVPCTransitGatewayServiceRolePolicy 3322
Menggunakan kebijakan ini 3323
Rincian kebijakan 3323
Versi kebijakan 3323
Dokumen kebijakan JSON 3323
Pelajari selengkapnya 3324
AWSVPCVerifiedAccessServiceRolePolicy 3324
Menggunakan kebijakan ini 3324
Rincian kebijakan 3324
Versi kebijakan 3324
Dokumen kebijakan JSON 3325
Pelajari selengkapnya 3326
AWSWAFConsoleFullAccess 3326
Menggunakan kebijakan ini 3327
Rincian kebijakan 3327
Versi kebijakan 3327
Dokumen kebijakan JSON 3327
Pelajari selengkapnya 3334
AWSWAFConsoleReadOnlyAccess 3334
Menggunakan kebijakan ini 3335
Rincian kebijakan 3335
Versi kebijakan 3335
Dokumen kebijakan JSON 3335
Pelajari selengkapnya 3340
AWSWAFFullAccess 3340
Menggunakan kebijakan ini 3340
Rincian kebijakan 3340
Versi kebijakan 3341
Dokumen kebijakan JSON 3341
Pelajari selengkapnya 3346
AWSWAFReadOnlyAccess 3346
Menggunakan kebijakan ini 3346
Rincian kebijakan 3346
Versi kebijakan 3346
Dokumen kebijakan JSON 3347
Pelajari selengkapnya 3350

AWSWellArchitectedDiscoveryServiceRolePolicy 3350
Menggunakan kebijakan ini 3350
Rincian kebijakan 3350
Versi kebijakan 3351
Dokumen kebijakan JSON 3351
Pelajari selengkapnya 3352
AWSWellArchitectedOrganizationsServiceRolePolicy 3352
Menggunakan kebijakan ini 3353
Rincian kebijakan 3353
Versi kebijakan 3353
Dokumen kebijakan JSON 3353
Pelajari selengkapnya 3354
AWSWickrFullAccess 3354
Menggunakan kebijakan ini 3354
Rincian kebijakan 3354
Versi kebijakan 3354
Dokumen kebijakan JSON 3355
Pelajari selengkapnya 3355
AWSXrayCrossAccountSharingConfiguration 3355
Menggunakan kebijakan ini 3355
Rincian kebijakan 3355
Versi kebijakan 3356
Dokumen kebijakan JSON 3356
Pelajari selengkapnya 3357
AWSXRayDaemonWriteAccess 3357
Menggunakan kebijakan ini 3357
Rincian kebijakan 3357
Versi kebijakan 3357
Dokumen kebijakan JSON 3358
Pelajari selengkapnya 3358
AWSXrayFullAccess 3358
Menggunakan kebijakan ini 3358
Rincian kebijakan 3359
Versi kebijakan 3359
Dokumen kebijakan JSON 3359
Pelajari selengkapnya 3359

AWSXrayReadOnlyAccess 3360
Menggunakan kebijakan ini 3360
Rincian kebijakan 3360
Versi kebijakan 3360
Dokumen kebijakan JSON 3360
Pelajari selengkapnya 3361
AWSXrayWriteOnlyAccess 3361
Menggunakan kebijakan ini 3361
Rincian kebijakan 3362
Versi kebijakan 3362
Dokumen kebijakan JSON 3362
Pelajari selengkapnya 3362
AWSZonalAutoshiftPracticeRunSLRPolicy 3363
Menggunakan kebijakan ini 3363
Rincian kebijakan 3363
Versi kebijakan 3363
Dokumen kebijakan JSON 3363
Pelajari selengkapnya 3364
AWSZoneGroupAccessManagementServiceRolePolicy 3365
Menggunakan kebijakan ini 3365
Rincian kebijakan 3365
Versi kebijakan 3365
Dokumen kebijakan JSON 3365
Pelajari selengkapnya 3366
BatchServiceRolePolicy 3366
Menggunakan kebijakan ini 3366
Rincian kebijakan 3366
Versi kebijakan 3367
Dokumen kebijakan JSON 3367
Pelajari selengkapnya 3373
Billing 3373
Menggunakan kebijakan ini 3373
Rincian kebijakan 3373
Versi kebijakan 3373
Dokumen kebijakan JSON 3374
Pelajari selengkapnya 3377

CertificateManagerServiceRolePolicy 3377
Menggunakan kebijakan ini 3378
Rincian kebijakan 3378
Versi kebijakan 3378
Dokumen kebijakan JSON 3378
Pelajari selengkapnya 3379
ClientVPNServiceConnectionsRolePolicy 3379
Menggunakan kebijakan ini 3379
Rincian kebijakan 3379
Versi kebijakan 3379
Dokumen kebijakan JSON 3379
Pelajari selengkapnya 3380
ClientVPNServiceRolePolicy 3380
Menggunakan kebijakan ini 3380
Rincian kebijakan 3380
Versi kebijakan 3380
Dokumen kebijakan JSON 3381
Pelajari selengkapnya 3381
CloudFormationStackSetsOrgAdminServiceRolePolicy 3382
Menggunakan kebijakan ini 3382
Rincian kebijakan 3382
Versi kebijakan 3382
Dokumen kebijakan JSON 3382
Pelajari selengkapnya 3383
CloudFormationStackSetsOrgMemberServiceRolePolicy 3383
Menggunakan kebijakan ini 3383
Rincian kebijakan 3383
Versi kebijakan 3384
Dokumen kebijakan JSON 3384
Pelajari selengkapnya 3385
CloudFrontFullAccess 3385
Menggunakan kebijakan ini 3385
Rincian kebijakan 3385
Versi kebijakan 3385
Dokumen kebijakan JSON 3385
Pelajari selengkapnya 3387

CloudFrontReadOnlyAccess 3387
Menggunakan kebijakan ini 3387
Rincian kebijakan 3387
Versi kebijakan 3388
Dokumen kebijakan JSON 3388
Pelajari selengkapnya 3389
CloudHSMServiceRolePolicy 3389
Menggunakan kebijakan ini 3389
Rincian kebijakan 3389
Versi kebijakan 3389
Dokumen kebijakan JSON 3389
Pelajari selengkapnya 3390
CloudSearchFullAccess 3390
Menggunakan kebijakan ini 3390
Rincian kebijakan 3390
Versi kebijakan 3391
Dokumen kebijakan JSON 3391
Pelajari selengkapnya 3391
CloudSearchReadOnlyAccess 3391
Menggunakan kebijakan ini 3391
Rincian kebijakan 3392
Versi kebijakan 3392
Dokumen kebijakan JSON 3392
Pelajari selengkapnya 3392
CloudTrailEventContext 3393
Menggunakan kebijakan ini 3393
Rincian kebijakan 3393
Versi kebijakan 3393
Dokumen kebijakan JSON 3393
Pelajari selengkapnya 3395
CloudTrailServiceRolePolicy 3395
Menggunakan kebijakan ini 3395
Rincian kebijakan 3395
Versi kebijakan 3396
Dokumen kebijakan JSON 3396
Pelajari selengkapnya 3397

CloudWatch-CrossAccountAccess 3398
Menggunakan kebijakan ini 3398
Rincian kebijakan 3398
Versi kebijakan 3398
Dokumen kebijakan JSON 3398
Pelajari selengkapnya 3399
CloudWatchActionsEC2Access 3399
Menggunakan kebijakan ini 3399
Rincian kebijakan 3399
Versi kebijakan 3399
Dokumen kebijakan JSON 3400
Pelajari selengkapnya 3400
CloudWatchAgentAdminPolicy 3400
Menggunakan kebijakan ini 3400
Rincian kebijakan 3400
Versi kebijakan 3401
Dokumen kebijakan JSON 3401
Pelajari selengkapnya 3402
CloudWatchAgentServerPolicy 3402
Menggunakan kebijakan ini 3402
Rincian kebijakan 3402
Versi kebijakan 3402
Dokumen kebijakan JSON 3403
Pelajari selengkapnya 3404
CloudWatchApplicationInsightsFullAccess 3404
Menggunakan kebijakan ini 3404
Rincian kebijakan 3404
Versi kebijakan 3404
Dokumen kebijakan JSON 3404
Pelajari selengkapnya 3406
CloudWatchApplicationInsightsReadOnlyAccess 3406
Menggunakan kebijakan ini 3406
Rincian kebijakan 3406
Versi kebijakan 3406
Dokumen kebijakan JSON 3407
Pelajari selengkapnya 3407

CloudwatchApplicationInsightsServiceLinkedRolePolicy 3407
Menggunakan kebijakan ini 3407
Rincian kebijakan 3408
Versi kebijakan 3408
Dokumen kebijakan JSON 3408
Pelajari selengkapnya 3418
CloudWatchApplicationSignalsFullAccess 3419
Menggunakan kebijakan ini 3419
Rincian kebijakan 3419
Versi kebijakan 3419
Dokumen kebijakan JSON 3419
Pelajari selengkapnya 3422
CloudWatchApplicationSignalsReadOnlyAccess 3422
Menggunakan kebijakan ini 3423
Rincian kebijakan 3423
Versi kebijakan 3423
Dokumen kebijakan JSON 3423
Pelajari selengkapnya 3425
CloudWatchApplicationSignalsServiceRolePolicy 3426
Menggunakan kebijakan ini 3426
Rincian kebijakan 3426
Versi kebijakan 3426
Dokumen kebijakan JSON 3426
Pelajari selengkapnya 3429
CloudWatchAutomaticDashboardsAccess 3429
Menggunakan kebijakan ini 3429
Rincian kebijakan 3429
Versi kebijakan 3430
Dokumen kebijakan JSON 3430
Pelajari selengkapnya 3431
CloudWatchCrossAccountSharingConfiguration 3431
Menggunakan kebijakan ini 3431
Rincian kebijakan 3432
Versi kebijakan 3432
Dokumen kebijakan JSON 3432
Pelajari selengkapnya 3433

CloudWatchEventsBuiltInTargetExecutionAccess 3433
Menggunakan kebijakan ini 3433
Rincian kebijakan 3433
Versi kebijakan 3434
Dokumen kebijakan JSON 3434
Pelajari selengkapnya 3434
CloudWatchEventsFullAccess 3434
Menggunakan kebijakan ini 3435
Rincian kebijakan 3435
Versi kebijakan 3435
Dokumen kebijakan JSON 3435
Pelajari selengkapnya 3437
CloudWatchEventsInvocationAccess 3437
Menggunakan kebijakan ini 3437
Rincian kebijakan 3438
Versi kebijakan 3438
Dokumen kebijakan JSON 3438
Pelajari selengkapnya 3438
CloudWatchEventsReadOnlyAccess 3439
Menggunakan kebijakan ini 3439
Rincian kebijakan 3439
Versi kebijakan 3439
Dokumen kebijakan JSON 3439
Pelajari selengkapnya 3441
CloudWatchEventsServiceRolePolicy 3441
Menggunakan kebijakan ini 3441
Rincian kebijakan 3441
Versi kebijakan 3441
Dokumen kebijakan JSON 3442
Pelajari selengkapnya 3442
CloudWatchFullAccess 3442
Menggunakan kebijakan ini 3442
Rincian kebijakan 3443
Versi kebijakan 3443
Dokumen kebijakan JSON 3443
Pelajari selengkapnya 3444

CloudWatchFullAccessV2 3444
Menggunakan kebijakan ini 3444
Rincian kebijakan 3444
Versi kebijakan 3445
Dokumen kebijakan JSON 3445
Pelajari selengkapnya 3446
CloudWatchInternetMonitorFullAccess 3447
Menggunakan kebijakan ini 3447
Rincian kebijakan 3447
Versi kebijakan 3447
Dokumen kebijakan JSON 3447
Pelajari selengkapnya 3449
CloudWatchInternetMonitorReadOnlyAccess 3449
Menggunakan kebijakan ini 3450
Rincian kebijakan 3450
Versi kebijakan 3450
Dokumen kebijakan JSON 3450
Pelajari selengkapnya 3451
CloudWatchInternetMonitorServiceRolePolicy 3451
Menggunakan kebijakan ini 3451
Rincian kebijakan 3451
Versi kebijakan 3452
Dokumen kebijakan JSON 3452
Pelajari selengkapnya 3453
CloudWatchLambdaApplicationSignalsExecutionRolePolicy 3453
Menggunakan kebijakan ini 3453
Rincian kebijakan 3453
Versi kebijakan 3453
Dokumen kebijakan JSON 3454
Pelajari selengkapnya 3455
CloudWatchLambdaInsightsExecutionRolePolicy 3455
Menggunakan kebijakan ini 3455
Rincian kebijakan 3455
Versi kebijakan 3455
Dokumen kebijakan JSON 3455
Pelajari selengkapnya 3456

CloudWatchLogsCrossAccountSharingConfiguration 3456
Menggunakan kebijakan ini 3456
Rincian kebijakan 3456
Versi kebijakan 3457
Dokumen kebijakan JSON 3457
Pelajari selengkapnya 3458
CloudWatchLogsFullAccess 3458
Menggunakan kebijakan ini 3458
Rincian kebijakan 3458
Versi kebijakan 3458
Dokumen kebijakan JSON 3459
Pelajari selengkapnya 3459
CloudWatchLogsReadOnlyAccess 3459
Menggunakan kebijakan ini 3459
Rincian kebijakan 3460
Versi kebijakan 3460
Dokumen kebijakan JSON 3460
Pelajari selengkapnya 3461
CloudWatchNetworkFlowMonitorAgentPublishPolicy 3461
Menggunakan kebijakan ini 3461
Rincian kebijakan 3461
Versi kebijakan 3461
Dokumen kebijakan JSON 3462
Pelajari selengkapnya 3462
CloudWatchNetworkFlowMonitorServiceRolePolicy 3462
Menggunakan kebijakan ini 3462
Rincian kebijakan 3463
Versi kebijakan 3463
Dokumen kebijakan JSON 3463
Pelajari selengkapnya 3464
CloudWatchNetworkFlowMonitorTopologyServiceRolePolicy 3464
Menggunakan kebijakan ini 3464
Rincian kebijakan 3464
Versi kebijakan 3465
Dokumen kebijakan JSON 3465
Pelajari selengkapnya 3466

CloudWatchNetworkMonitorServiceRolePolicy 3466
Menggunakan kebijakan ini 3466
Rincian kebijakan 3466
Versi kebijakan 3466
Dokumen kebijakan JSON 3467
Pelajari selengkapnya 3468
CloudWatchOpenSearchDashboardAccess 3468
Menggunakan kebijakan ini 3468
Rincian kebijakan 3468
Versi kebijakan 3468
Dokumen kebijakan JSON 3469
Pelajari selengkapnya 3471
CloudWatchOpenSearchDashboardsFullAccess 3471
Menggunakan kebijakan ini 3471
Rincian kebijakan 3472
Versi kebijakan 3472
Dokumen kebijakan JSON 3472
Pelajari selengkapnya 3479
CloudWatchReadOnlyAccess 3479
Menggunakan kebijakan ini 3479
Rincian kebijakan 3479
Versi kebijakan 3480
Dokumen kebijakan JSON 3480
Pelajari selengkapnya 3481
CloudWatchSyntheticsFullAccess 3481
Menggunakan kebijakan ini 3482
Rincian kebijakan 3482
Versi kebijakan 3482
Dokumen kebijakan JSON 3482
Pelajari selengkapnya 3487
CloudWatchSyntheticsReadOnlyAccess 3487
Menggunakan kebijakan ini 3488
Rincian kebijakan 3488
Versi kebijakan 3488
Dokumen kebijakan JSON 3488
Pelajari selengkapnya 3489

ComprehendDataAccessRolePolicy 3489
Menggunakan kebijakan ini 3489
Rincian kebijakan 3489
Versi kebijakan 3489
Dokumen kebijakan JSON 3489
Pelajari selengkapnya 3490
ComprehendFullAccess 3490
Menggunakan kebijakan ini 3490
Rincian kebijakan 3490
Versi kebijakan 3491
Dokumen kebijakan JSON 3491
Pelajari selengkapnya 3491
ComprehendMedicalFullAccess 3491
Menggunakan kebijakan ini 3492
Rincian kebijakan 3492
Versi kebijakan 3492
Dokumen kebijakan JSON 3492
Pelajari selengkapnya 3492
ComprehendReadOnly 3493
Menggunakan kebijakan ini 3493
Rincian kebijakan 3493
Versi kebijakan 3493
Dokumen kebijakan JSON 3493
Pelajari selengkapnya 3495
ComputeOptimizerReadOnlyAccess 3495
Menggunakan kebijakan ini 3495
Rincian kebijakan 3495
Versi kebijakan 3495
Dokumen kebijakan JSON 3495
Pelajari selengkapnya 3497
ComputeOptimizerServiceRolePolicy 3497
Menggunakan kebijakan ini 3497
Rincian kebijakan 3497
Versi kebijakan 3497
Dokumen kebijakan JSON 3498
Pelajari selengkapnya 3499

ConfigConformsServiceRolePolicy 3499
Menggunakan kebijakan ini 3499
Rincian kebijakan 3499
Versi kebijakan 3500
Dokumen kebijakan JSON 3500
Pelajari selengkapnya 3502
CostOptimizationHubAdminAccess 3503
Menggunakan kebijakan ini 3503
Rincian kebijakan 3503
Versi kebijakan 3503
Dokumen kebijakan JSON 3503
Pelajari selengkapnya 3505
CostOptimizationHubReadOnlyAccess 3505
Menggunakan kebijakan ini 3505
Rincian kebijakan 3505
Versi kebijakan 3505
Dokumen kebijakan JSON 3505
Pelajari selengkapnya 3506
CostOptimizationHubServiceRolePolicy 3506
Menggunakan kebijakan ini 3506
Rincian kebijakan 3506
Versi kebijakan 3507
Dokumen kebijakan JSON 3507
Pelajari selengkapnya 3508
CustomerProfilesServiceLinkedRolePolicy 3508
Menggunakan kebijakan ini 3508
Rincian kebijakan 3508
Versi kebijakan 3509
Dokumen kebijakan JSON 3509
Pelajari selengkapnya 3510
DatabaseAdministrator 3510
Menggunakan kebijakan ini 3510
Rincian kebijakan 3510
Versi kebijakan 3511
Dokumen kebijakan JSON 3511
Pelajari selengkapnya 3513

DataScientist 3513
Menggunakan kebijakan ini 3513
Rincian kebijakan 3514
Versi kebijakan 3514
Dokumen kebijakan JSON 3514
Pelajari selengkapnya 3518
DAXServiceRolePolicy 3518
Menggunakan kebijakan ini 3518
Rincian kebijakan 3518
Versi kebijakan 3518
Dokumen kebijakan JSON 3519
Pelajari selengkapnya 3519
DeclarativePoliciesEC2Report 3519
Menggunakan kebijakan ini 3520
Rincian kebijakan 3520
Versi kebijakan 3520
Dokumen kebijakan JSON 3520
Pelajari selengkapnya 3521
DynamoDBCloudWatchContributorInsightsServiceRolePolicy 3521
Menggunakan kebijakan ini 3521
Rincian kebijakan 3521
Versi kebijakan 3521
Dokumen kebijakan JSON 3522
Pelajari selengkapnya 3522
DynamoDBKinesisReplicationServiceRolePolicy 3522
Menggunakan kebijakan ini 3523
Rincian kebijakan 3523
Versi kebijakan 3523
Dokumen kebijakan JSON 3523
Pelajari selengkapnya 3524
DynamoDBReplicationServiceRolePolicy 3524
Menggunakan kebijakan ini 3524
Rincian kebijakan 3524
Versi kebijakan 3524
Dokumen kebijakan JSON 3525
Pelajari selengkapnya 3526

EC2FastLaunchFullAccess 3526
Menggunakan kebijakan ini 3526
Rincian kebijakan 3526
Versi kebijakan 3526
Dokumen kebijakan JSON 3527
Pelajari selengkapnya 3534
EC2FastLaunchServiceRolePolicy 3534
Menggunakan kebijakan ini 3534
Rincian kebijakan 3534
Versi kebijakan 3534
Dokumen kebijakan JSON 3535
Pelajari selengkapnya 3540
EC2FleetTimeShiftableServiceRolePolicy 3540
Menggunakan kebijakan ini 3540
Rincian kebijakan 3540
Versi kebijakan 3540
Dokumen kebijakan JSON 3541
Pelajari selengkapnya 3542
Ec2ImageBuilderCrossAccountDistributionAccess 3542
Menggunakan kebijakan ini 3542
Rincian kebijakan 3542
Versi kebijakan 3543
Dokumen kebijakan JSON 3543
Pelajari selengkapnya 3543
EC2ImageBuilderLifecycleExecutionPolicy 3544
Menggunakan kebijakan ini 3544
Rincian kebijakan 3544
Versi kebijakan 3544
Dokumen kebijakan JSON 3544
Pelajari selengkapnya 3546
EC2InstanceConnect 3547
Menggunakan kebijakan ini 3547
Rincian kebijakan 3547
Versi kebijakan 3547
Dokumen kebijakan JSON 3547
Pelajari selengkapnya 3548

Ec2InstanceConnectEndpoint 3548
Menggunakan kebijakan ini 3548
Rincian kebijakan 3548
Versi kebijakan 3548
Dokumen kebijakan JSON 3549
Pelajari selengkapnya 3551
EC2InstanceProfileForImageBuilder 3551
Menggunakan kebijakan ini 3551
Rincian kebijakan 3551
Versi kebijakan 3551
Dokumen kebijakan JSON 3551
Pelajari selengkapnya 3554
EC2InstanceProfileForImageBuilderECRContainerBuilds 3554
Menggunakan kebijakan ini 3555
Rincian kebijakan 3555
Versi kebijakan 3555
Dokumen kebijakan JSON 3555
Pelajari selengkapnya 3556
ECRReplicationServiceRolePolicy 3557
Menggunakan kebijakan ini 3557
Rincian kebijakan 3557
Versi kebijakan 3557
Dokumen kebijakan JSON 3557
Pelajari selengkapnya 3558
ECRTemplateServiceRolePolicy 3558
Menggunakan kebijakan ini 3558
Rincian kebijakan 3558
Versi kebijakan 3558
Dokumen kebijakan JSON 3559
Pelajari selengkapnya 3559
ElastiCacheServiceRolePolicy 3559
Menggunakan kebijakan ini 3559
Rincian kebijakan 3560
Versi kebijakan 3560
Dokumen kebijakan JSON 3560
Pelajari selengkapnya 3562

ElasticLoadBalancingFullAccess 3562
Menggunakan kebijakan ini 3562
Rincian kebijakan 3562
Versi kebijakan 3563
Dokumen kebijakan JSON 3563
Pelajari selengkapnya 3564
ElasticLoadBalancingReadOnly 3564
Menggunakan kebijakan ini 3564
Rincian kebijakan 3565
Versi kebijakan 3565
Dokumen kebijakan JSON 3565
Pelajari selengkapnya 3566
ElementalActivationsDownloadSoftwareAccess 3566
Menggunakan kebijakan ini 3566
Rincian kebijakan 3566
Versi kebijakan 3567
Dokumen kebijakan JSON 3567
Pelajari selengkapnya 3567
ElementalActivationsFullAccess 3568
Menggunakan kebijakan ini 3568
Rincian kebijakan 3568
Versi kebijakan 3568
Dokumen kebijakan JSON 3568
Pelajari selengkapnya 3569
ElementalActivationsGenerateLicenses 3569
Menggunakan kebijakan ini 3569
Rincian kebijakan 3569
Versi kebijakan 3569
Dokumen kebijakan JSON 3570
Pelajari selengkapnya 3570
ElementalActivationsReadOnlyAccess 3570
Menggunakan kebijakan ini 3570
Rincian kebijakan 3571
Versi kebijakan 3571
Dokumen kebijakan JSON 3571
Pelajari selengkapnya 3571

ElementalAppliancesSoftwareFullAccess 3572
Menggunakan kebijakan ini 3572
Rincian kebijakan 3572
Versi kebijakan 3572
Dokumen kebijakan JSON 3572
Pelajari selengkapnya 3573
ElementalAppliancesSoftwareReadOnlyAccess 3573
Menggunakan kebijakan ini 3573
Rincian kebijakan 3573
Versi kebijakan 3573
Dokumen kebijakan JSON 3574
Pelajari selengkapnya 3574
ElementalSupportCenterFullAccess 3574
Menggunakan kebijakan ini 3574
Rincian kebijakan 3575
Versi kebijakan 3575
Dokumen kebijakan JSON 3575
Pelajari selengkapnya 3575
EMRDescribeClusterPolicyForEMRWAL 3576
Menggunakan kebijakan ini 3576
Rincian kebijakan 3576
Versi kebijakan 3576
Dokumen kebijakan JSON 3576
Pelajari selengkapnya 3577
FMSServiceRolePolicy 3577
Menggunakan kebijakan ini 3577
Rincian kebijakan 3577
Versi kebijakan 3577
Dokumen kebijakan JSON 3578
Pelajari selengkapnya 3594
FSxDeleteServiceLinkedRoleAccess 3594
Menggunakan kebijakan ini 3594
Rincian kebijakan 3594
Versi kebijakan 3595
Dokumen kebijakan JSON 3595
Pelajari selengkapnya 3595

GameLiftContainerFleetPolicy 3596
Menggunakan kebijakan ini 3596
Rincian kebijakan 3596
Versi kebijakan 3596
Dokumen kebijakan JSON 3596
Pelajari selengkapnya 3597
GameLiftGameServerGroupPolicy 3598
Menggunakan kebijakan ini 3598
Rincian kebijakan 3598
Versi kebijakan 3598
Dokumen kebijakan JSON 3598
Pelajari selengkapnya 3600
GitLabDuoWithAmazonQPermissionsPolicy 3600
Menggunakan kebijakan ini 3600
Rincian kebijakan 3600
Versi kebijakan 3601
Dokumen kebijakan JSON 3601
Pelajari selengkapnya 3602
GlobalAcceleratorFullAccess 3602
Menggunakan kebijakan ini 3602
Rincian kebijakan 3602
Versi kebijakan 3602
Dokumen kebijakan JSON 3603
Pelajari selengkapnya 3604
GlobalAcceleratorReadOnlyAccess 3604
Menggunakan kebijakan ini 3604
Rincian kebijakan 3604
Versi kebijakan 3604
Dokumen kebijakan JSON 3604
Pelajari selengkapnya 3605
GreengrassOTAUpdateArtifactAccess 3605
Menggunakan kebijakan ini 3605
Rincian kebijakan 3605
Versi kebijakan 3606
Dokumen kebijakan JSON 3606
Pelajari selengkapnya 3606

GroundTruthSyntheticConsoleFullAccess 3606
Menggunakan kebijakan ini 3607
Rincian kebijakan 3607
Versi kebijakan 3607
Dokumen kebijakan JSON 3607
Pelajari selengkapnya 3607
GroundTruthSyntheticConsoleReadOnlyAccess 3608
Menggunakan kebijakan ini 3608
Rincian kebijakan 3608
Versi kebijakan 3608
Dokumen kebijakan JSON 3608
Pelajari selengkapnya 3609
Health_OrganizationsServiceRolePolicy 3609
Menggunakan kebijakan ini 3609
Rincian kebijakan 3609
Versi kebijakan 3610
Dokumen kebijakan JSON 3610
Pelajari selengkapnya 3610
IAMAccessAdvisorReadOnly 3610
Menggunakan kebijakan ini 3611
Rincian kebijakan 3611
Versi kebijakan 3611
Dokumen kebijakan JSON 3611
Pelajari selengkapnya 3612
IAMAccessAnalyzerFullAccess 3612
Menggunakan kebijakan ini 3612
Rincian kebijakan 3612
Versi kebijakan 3613
Dokumen kebijakan JSON 3613
Pelajari selengkapnya 3614
IAMAccessAnalyzerReadOnlyAccess 3614
Menggunakan kebijakan ini 3614
Rincian kebijakan 3614
Versi kebijakan 3614
Dokumen kebijakan JSON 3615
Pelajari selengkapnya 3615

IAMFullAccess 3615
Menggunakan kebijakan ini 3616
Rincian kebijakan 3616
Versi kebijakan 3616
Dokumen kebijakan JSON 3616
Pelajari selengkapnya 3617
IAMReadOnlyAccess 3617
Menggunakan kebijakan ini 3617
Rincian kebijakan 3617
Versi kebijakan 3617
Dokumen kebijakan JSON 3618
Pelajari selengkapnya 3618
IAMSelfManageServiceSpecificCredentials 3618
Menggunakan kebijakan ini 3618
Rincian kebijakan 3619
Versi kebijakan 3619
Dokumen kebijakan JSON 3619
Pelajari selengkapnya 3619
IAMUserChangePassword 3620
Menggunakan kebijakan ini 3620
Rincian kebijakan 3620
Versi kebijakan 3620
Dokumen kebijakan JSON 3620
Pelajari selengkapnya 3621
IAMUserSSHKeys 3621
Menggunakan kebijakan ini 3621
Rincian kebijakan 3621
Versi kebijakan 3622
Dokumen kebijakan JSON 3622
Pelajari selengkapnya 3622
IVSFullAccess 3622
Menggunakan kebijakan ini 3623
Rincian kebijakan 3623
Versi kebijakan 3623
Dokumen kebijakan JSON 3623
Pelajari selengkapnya 3624

IVSReadOnlyAccess 3624
Menggunakan kebijakan ini 3624
Rincian kebijakan 3624
Versi kebijakan 3624
Dokumen kebijakan JSON 3624
Pelajari selengkapnya 3626
IVSRecordToS3 3626
Menggunakan kebijakan ini 3626
Rincian kebijakan 3626
Versi kebijakan 3626
Dokumen kebijakan JSON 3627
Pelajari selengkapnya 3627
KafkaConnectServiceRolePolicy 3627
Menggunakan kebijakan ini 3627
Rincian kebijakan 3627
Versi kebijakan 3628
Dokumen kebijakan JSON 3628
Pelajari selengkapnya 3629
KafkaServiceRolePolicy 3629
Menggunakan kebijakan ini 3630
Rincian kebijakan 3630
Versi kebijakan 3630
Dokumen kebijakan JSON 3630
Pelajari selengkapnya 3632
KeyspacesCDCServiceRolePolicy 3632
Menggunakan kebijakan ini 3632
Rincian kebijakan 3632
Versi kebijakan 3632
Dokumen kebijakan JSON 3632
Pelajari selengkapnya 3633
KeyspacesReplicationServiceRolePolicy 3633
Menggunakan kebijakan ini 3633
Rincian kebijakan 3633
Versi kebijakan 3634
Dokumen kebijakan JSON 3634
Pelajari selengkapnya 3635

LakeFormationDataAccessServiceRolePolicy 3635
Menggunakan kebijakan ini 3636
Rincian kebijakan 3636
Versi kebijakan 3636
Dokumen kebijakan JSON 3636
Pelajari selengkapnya 3637
LexBotPolicy 3637
Menggunakan kebijakan ini 3637
Rincian kebijakan 3637
Versi kebijakan 3637
Dokumen kebijakan JSON 3637
Pelajari selengkapnya 3638
LexChannelPolicy 3638
Menggunakan kebijakan ini 3638
Rincian kebijakan 3638
Versi kebijakan 3639
Dokumen kebijakan JSON 3639
Pelajari selengkapnya 3639
LightsailExportAccess 3639
Menggunakan kebijakan ini 3640
Rincian kebijakan 3640
Versi kebijakan 3640
Dokumen kebijakan JSON 3640
Pelajari selengkapnya 3641
MediaConnectGatewayInstanceRolePolicy 3641
Menggunakan kebijakan ini 3641
Rincian kebijakan 3641
Versi kebijakan 3642
Dokumen kebijakan JSON 3642
Pelajari selengkapnya 3642
MediaPackageServiceRolePolicy 3642
Menggunakan kebijakan ini 3643
Rincian kebijakan 3643
Versi kebijakan 3643
Dokumen kebijakan JSON 3643
Pelajari selengkapnya 3644

MemoryDBServiceRolePolicy 3644
Menggunakan kebijakan ini 3644
Rincian kebijakan 3644
Versi kebijakan 3644
Dokumen kebijakan JSON 3645
Pelajari selengkapnya 3647
MigrationHubDMSAccessServiceRolePolicy 3647
Menggunakan kebijakan ini 3647
Rincian kebijakan 3647
Versi kebijakan 3647
Dokumen kebijakan JSON 3648
Pelajari selengkapnya 3649
MigrationHubServiceRolePolicy 3649
Menggunakan kebijakan ini 3649
Rincian kebijakan 3649
Versi kebijakan 3649
Dokumen kebijakan JSON 3649
Pelajari selengkapnya 3651
MigrationHubSMSAccessServiceRolePolicy 3651
Menggunakan kebijakan ini 3651
Rincian kebijakan 3651
Versi kebijakan 3651
Dokumen kebijakan JSON 3652
Pelajari selengkapnya 3652
MonitronServiceRolePolicy 3653
Menggunakan kebijakan ini 3653
Rincian kebijakan 3653
Versi kebijakan 3653
Dokumen kebijakan JSON 3653
Pelajari selengkapnya 3654
MultiPartyApprovalFullAccess 3654
Menggunakan kebijakan ini 3654
Rincian kebijakan 3654
Versi kebijakan 3654
Dokumen kebijakan JSON 3655
Pelajari selengkapnya 3656

MultiPartyApprovalReadOnlyAccess 3656
Menggunakan kebijakan ini 3657
Rincian kebijakan 3657
Versi kebijakan 3657
Dokumen kebijakan JSON 3657
Pelajari selengkapnya 3658
NeptuneConsoleFullAccess 3658
Menggunakan kebijakan ini 3659
Rincian kebijakan 3659
Versi kebijakan 3659
Dokumen kebijakan JSON 3659
Pelajari selengkapnya 3665
NeptuneFullAccess 3665
Menggunakan kebijakan ini 3665
Rincian kebijakan 3665
Versi kebijakan 3665
Dokumen kebijakan JSON 3665
Pelajari selengkapnya 3669
NeptuneGraphReadOnlyAccess 3670
Menggunakan kebijakan ini 3670
Rincian kebijakan 3670
Versi kebijakan 3670
Dokumen kebijakan JSON 3670
Pelajari selengkapnya 3672
NeptuneReadOnlyAccess 3672
Menggunakan kebijakan ini 3672
Rincian kebijakan 3672
Versi kebijakan 3672
Dokumen kebijakan JSON 3673
Pelajari selengkapnya 3675
NetworkAdministrator 3675
Menggunakan kebijakan ini 3675
Rincian kebijakan 3675
Versi kebijakan 3675
Dokumen kebijakan JSON 3676
Pelajari selengkapnya 3683

NetworkSecurityDirectorServiceLinkedRolePolicy 3683
Menggunakan kebijakan ini 3683
Rincian kebijakan 3683
Versi kebijakan 3683
Dokumen kebijakan JSON 3684
Pelajari selengkapnya 3687
OAMFullAccess 3687
Menggunakan kebijakan ini 3687
Rincian kebijakan 3688
Versi kebijakan 3688
Dokumen kebijakan JSON 3688
Pelajari selengkapnya 3688
OAMReadOnlyAccess 3689
Menggunakan kebijakan ini 3689
Rincian kebijakan 3689
Versi kebijakan 3689
Dokumen kebijakan JSON 3689
Pelajari selengkapnya 3690
OpensearchIngestionSelfManagedVpcePolicy 3690
Menggunakan kebijakan ini 3690
Rincian kebijakan 3690
Versi kebijakan 3690
Dokumen kebijakan JSON 3691
Pelajari selengkapnya 3691
PartnerCentralAccountManagementUserRoleAssociation 3691
Menggunakan kebijakan ini 3692
Rincian kebijakan 3692
Versi kebijakan 3692
Dokumen kebijakan JSON 3692
Pelajari selengkapnya 3693
PowerUserAccess 3693
Menggunakan kebijakan ini 3693
Rincian kebijakan 3693
Versi kebijakan 3694
Dokumen kebijakan JSON 3694
Pelajari selengkapnya 3694

QAppsServiceRolePolicy 3695
Menggunakan kebijakan ini 3695
Rincian kebijakan 3695
Versi kebijakan 3695
Dokumen kebijakan JSON 3695
Pelajari selengkapnya 3696
QBusinessQuicksightPluginPolicy 3696
Menggunakan kebijakan ini 3696
Rincian kebijakan 3696
Versi kebijakan 3697
Dokumen kebijakan JSON 3697
Pelajari selengkapnya 3697
QBusinessServiceRolePolicy 3697
Menggunakan kebijakan ini 3698
Rincian kebijakan 3698
Versi kebijakan 3698
Dokumen kebijakan JSON 3698
Pelajari selengkapnya 3700
QuickSightAccessForS3StorageManagementAnalyticsReadOnly 3700
Menggunakan kebijakan ini 3700
Rincian kebijakan 3700
Versi kebijakan 3700
Dokumen kebijakan JSON 3701
Pelajari selengkapnya 3701
RDSCloudHsmAuthorizationRole 3701
Menggunakan kebijakan ini 3702
Rincian kebijakan 3702
Versi kebijakan 3702
Dokumen kebijakan JSON 3702
Pelajari selengkapnya 3703
ReadOnlyAccess 3703
Menggunakan kebijakan ini 3703
Rincian kebijakan 3703
Versi kebijakan 3703
Dokumen kebijakan JSON 3703
Pelajari selengkapnya 3759

ResourceGroupsandTagEditorFullAccess 3759
Menggunakan kebijakan ini 3759
Rincian kebijakan 3759
Versi kebijakan 3760
Dokumen kebijakan JSON 3760
Pelajari selengkapnya 3760
ResourceGroupsandTagEditorReadOnlyAccess 3761
Menggunakan kebijakan ini 3761
Rincian kebijakan 3761
Versi kebijakan 3761
Dokumen kebijakan JSON 3761
Pelajari selengkapnya 3762
ResourceGroupsServiceRolePolicy 3762
Menggunakan kebijakan ini 3762
Rincian kebijakan 3762
Versi kebijakan 3763
Dokumen kebijakan JSON 3763
Pelajari selengkapnya 3763
ResourceGroupsTaggingAPITagUntagSupportedResources 3763
Menggunakan kebijakan ini 3764
Rincian kebijakan 3764
Versi kebijakan 3764
Dokumen kebijakan JSON 3764
Pelajari selengkapnya 3772
ROSAAmazonEBSCSIDriverOperatorPolicy 3773
Menggunakan kebijakan ini 3773
Rincian kebijakan 3773
Versi kebijakan 3773
Dokumen kebijakan JSON 3773
Pelajari selengkapnya 3776
ROSACloudNetworkConfigOperatorPolicy 3777
Menggunakan kebijakan ini 3777
Rincian kebijakan 3777
Versi kebijakan 3777
Dokumen kebijakan JSON 3778
Pelajari selengkapnya 3778

ROSAControlPlaneOperatorPolicy 3779
Menggunakan kebijakan ini 3779
Rincian kebijakan 3779
Versi kebijakan 3779
Dokumen kebijakan JSON 3779
Pelajari selengkapnya 3784
ROSAImageRegistryOperatorPolicy 3784
Menggunakan kebijakan ini 3784
Rincian kebijakan 3784
Versi kebijakan 3784
Dokumen kebijakan JSON 3785
Pelajari selengkapnya 3786
ROSAIngressOperatorPolicy 3786
Menggunakan kebijakan ini 3786
Rincian kebijakan 3786
Versi kebijakan 3787
Dokumen kebijakan JSON 3787
Pelajari selengkapnya 3788
ROSAInstallerPolicy 3788
Menggunakan kebijakan ini 3788
Rincian kebijakan 3788
Versi kebijakan 3788
Dokumen kebijakan JSON 3789
Pelajari selengkapnya 3796
ROSAKMSProviderPolicy 3797
Menggunakan kebijakan ini 3797
Rincian kebijakan 3797
Versi kebijakan 3797
Dokumen kebijakan JSON 3797
Pelajari selengkapnya 3798
ROSAKubeControllerPolicy 3798
Menggunakan kebijakan ini 3798
Rincian kebijakan 3798
Versi kebijakan 3799
Dokumen kebijakan JSON 3799
Pelajari selengkapnya 3803

ROSAManageSubscription 3803
Menggunakan kebijakan ini 3804
Rincian kebijakan 3804
Versi kebijakan 3804
Dokumen kebijakan JSON 3804
Pelajari selengkapnya 3805
ROSANodePoolManagementPolicy 3805
Menggunakan kebijakan ini 3805
Rincian kebijakan 3805
Versi kebijakan 3806
Dokumen kebijakan JSON 3806
Pelajari selengkapnya 3812
ROSASRESupportPolicy 3812
Menggunakan kebijakan ini 3812
Rincian kebijakan 3812
Versi kebijakan 3812
Dokumen kebijakan JSON 3813
Pelajari selengkapnya 3817
ROSAWorkerInstancePolicy 3818
Menggunakan kebijakan ini 3818
Rincian kebijakan 3818
Versi kebijakan 3818
Dokumen kebijakan JSON 3818
Pelajari selengkapnya 3819
Route53RecoveryReadinessServiceRolePolicy 3820
Menggunakan kebijakan ini 3820
Rincian kebijakan 3820
Versi kebijakan 3820
Dokumen kebijakan JSON 3820
Pelajari selengkapnya 3824
Route53ResolverServiceRolePolicy 3824
Menggunakan kebijakan ini 3824
Rincian kebijakan 3824
Versi kebijakan 3824
Dokumen kebijakan JSON 3825
Pelajari selengkapnya 3825

S3StorageLensServiceRolePolicy 3825
Menggunakan kebijakan ini 3826
Rincian kebijakan 3826
Versi kebijakan 3826
Dokumen kebijakan JSON 3826
Pelajari selengkapnya 3827
SageMakerStudioAdminProjectUserRolePolicy 3827
Menggunakan kebijakan ini 3827
Rincian kebijakan 3827
Versi kebijakan 3827
Dokumen kebijakan JSON 3828
Pelajari selengkapnya 3830
SageMakerStudioBedrockAgentServiceRolePolicy 3830
Menggunakan kebijakan ini 3830
Rincian kebijakan 3830
Versi kebijakan 3831
Dokumen kebijakan JSON 3831
Pelajari selengkapnya 3834
SageMakerStudioBedrockChatAgentUserRolePolicy 3834
Menggunakan kebijakan ini 3835
Rincian kebijakan 3835
Versi kebijakan 3835
Dokumen kebijakan JSON 3835
Pelajari selengkapnya 3839
SageMakerStudioBedrockEvaluationJobServiceRolePolicy 3839
Menggunakan kebijakan ini 3840
Rincian kebijakan 3840
Versi kebijakan 3840
Dokumen kebijakan JSON 3840
Pelajari selengkapnya 3844
SageMakerStudioBedrockFlowServiceRolePolicy 3844
Menggunakan kebijakan ini 3844
Rincian kebijakan 3844
Versi kebijakan 3844
Dokumen kebijakan JSON 3845
Pelajari selengkapnya 3848

SageMakerStudioBedrockFunctionExecutionRolePolicy 3849
Menggunakan kebijakan ini 3849
Rincian kebijakan 3849
Versi kebijakan 3849
Dokumen kebijakan JSON 3849
Pelajari selengkapnya 3850
SageMakerStudioBedrockKnowledgeBaseCustomResourcePolicy 3851
Menggunakan kebijakan ini 3851
Rincian kebijakan 3851
Versi kebijakan 3851
Dokumen kebijakan JSON 3851
Pelajari selengkapnya 3852
SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy 3852
Menggunakan kebijakan ini 3853
Rincian kebijakan 3853
Versi kebijakan 3853
Dokumen kebijakan JSON 3853
Pelajari selengkapnya 3857
SageMakerStudioBedrockPromptUserRolePolicy 3857
Menggunakan kebijakan ini 3857
Rincian kebijakan 3857
Versi kebijakan 3857
Dokumen kebijakan JSON 3858
Pelajari selengkapnya 3860
SageMakerStudioDomainExecutionRolePolicy 3860
Menggunakan kebijakan ini 3860
Rincian kebijakan 3861
Versi kebijakan 3861
Dokumen kebijakan JSON 3861
Pelajari selengkapnya 3867
SageMakerStudioDomainServiceRolePolicy 3867
Menggunakan kebijakan ini 3867
Rincian kebijakan 3867
Versi kebijakan 3868
Dokumen kebijakan JSON 3868
Pelajari selengkapnya 3869

SageMakerStudioEMRInstanceRolePolicy 3869
Menggunakan kebijakan ini 3869
Rincian kebijakan 3869
Versi kebijakan 3869
Dokumen kebijakan JSON 3870
Pelajari selengkapnya 3873
SageMakerStudioEMRServiceRolePolicy 3873
Menggunakan kebijakan ini 3873
Rincian kebijakan 3873
Versi kebijakan 3874
Dokumen kebijakan JSON 3874
Pelajari selengkapnya 3877
SageMakerStudioFullAccess 3877
Menggunakan kebijakan ini 3877
Rincian kebijakan 3877
Versi kebijakan 3877
Dokumen kebijakan JSON 3877
Pelajari selengkapnya 3887
SageMakerStudioProjectProvisioningRolePolicy 3887
Menggunakan kebijakan ini 3887
Rincian kebijakan 3887
Versi kebijakan 3887
Dokumen kebijakan JSON 3888
Pelajari selengkapnya 3955
SageMakerStudioProjectRoleMachineLearningPolicy 3955
Menggunakan kebijakan ini 3955
Rincian kebijakan 3955
Versi kebijakan 3956
Dokumen kebijakan JSON 3956
Pelajari selengkapnya 3978
SageMakerStudioProjectUserRolePermissionsBoundary 3978
Menggunakan kebijakan ini 3978
Rincian kebijakan 3978
Versi kebijakan 3979
Dokumen kebijakan JSON 3979
Pelajari selengkapnya 4034

SageMakerStudioProjectUserRolePolicy 4034
Menggunakan kebijakan ini 4035
Rincian kebijakan 4035
Versi kebijakan 4035
Dokumen kebijakan JSON 4035
Pelajari selengkapnya 4096
SageMakerStudioQueryExecutionRolePolicy 4096
Menggunakan kebijakan ini 4097
Rincian kebijakan 4097
Versi kebijakan 4097
Dokumen kebijakan JSON 4097
Pelajari selengkapnya 4099
SecretsManagerReadWrite 4099
Menggunakan kebijakan ini 4099
Rincian kebijakan 4099
Versi kebijakan 4100
Dokumen kebijakan JSON 4100
Pelajari selengkapnya 4101
SecurityAudit 4102
Menggunakan kebijakan ini 4102
Rincian kebijakan 4102
Versi kebijakan 4102
Dokumen kebijakan JSON 4102
Pelajari selengkapnya 4123
SecurityLakeResourceManagementServiceRolePolicy 4123
Menggunakan kebijakan ini 4123
Rincian kebijakan 4123
Versi kebijakan 4124
Dokumen kebijakan JSON 4124
Pelajari selengkapnya 4129
SecurityLakeServiceLinkedRole 4129
Menggunakan kebijakan ini 4129
Rincian kebijakan 4129
Versi kebijakan 4130
Dokumen kebijakan JSON 4130
Pelajari selengkapnya 4133

ServerMigration_ServiceRole 4133
Menggunakan kebijakan ini 4133
Rincian kebijakan 4133
Versi kebijakan 4133
Dokumen kebijakan JSON 4133
Pelajari selengkapnya 4138
ServerMigrationConnector 4138
Menggunakan kebijakan ini 4139
Rincian kebijakan 4139
Versi kebijakan 4139
Dokumen kebijakan JSON 4139
Pelajari selengkapnya 4141
ServerMigrationServiceConsoleFullAccess 4141
Menggunakan kebijakan ini 4141
Rincian kebijakan 4141
Versi kebijakan 4141
Dokumen kebijakan JSON 4142
Pelajari selengkapnya 4143
ServerMigrationServiceLaunchRole 4143
Menggunakan kebijakan ini 4144
Rincian kebijakan 4144
Versi kebijakan 4144
Dokumen kebijakan JSON 4144
Pelajari selengkapnya 4147
ServerMigrationServiceRoleForInstanceValidation 4147
Menggunakan kebijakan ini 4147
Rincian kebijakan 4147
Versi kebijakan 4148
Dokumen kebijakan JSON 4148
Pelajari selengkapnya 4148
ServiceQuotasFullAccess 4148
Menggunakan kebijakan ini 4149
Rincian kebijakan 4149
Versi kebijakan 4149
Dokumen kebijakan JSON 4149
Pelajari selengkapnya 4151

ServiceQuotasReadOnlyAccess 4151
Menggunakan kebijakan ini 4151
Rincian kebijakan 4151
Versi kebijakan 4151
Dokumen kebijakan JSON 4152
Pelajari selengkapnya 4153
ServiceQuotasServiceRolePolicy 4153
Menggunakan kebijakan ini 4153
Rincian kebijakan 4153
Versi kebijakan 4153
Dokumen kebijakan JSON 4154
Pelajari selengkapnya 4154
SimpleWorkflowFullAccess 4154
Menggunakan kebijakan ini 4154
Rincian kebijakan 4154
Versi kebijakan 4155
Dokumen kebijakan JSON 4155
Pelajari selengkapnya 4155
SMSVoiceServiceRolePolicy 4155
Menggunakan kebijakan ini 4156
Rincian kebijakan 4156
Versi kebijakan 4156
Dokumen kebijakan JSON 4156
Pelajari selengkapnya 4157
SplitCostAllocationDataServiceRolePolicy 4157
Menggunakan kebijakan ini 4157
Rincian kebijakan 4157
Versi kebijakan 4157
Dokumen kebijakan JSON 4158
Pelajari selengkapnya 4158
SSMQuickSetupRolePolicy 4158
Menggunakan kebijakan ini 4159
Rincian kebijakan 4159
Versi kebijakan 4159
Dokumen kebijakan JSON 4159
Pelajari selengkapnya 4162

SupportUser 4162
Menggunakan kebijakan ini 4162
Rincian kebijakan 4162
Versi kebijakan 4163
Dokumen kebijakan JSON 4163
Pelajari selengkapnya 4168
SystemAdministrator 4168
Menggunakan kebijakan ini 4168
Rincian kebijakan 4168
Versi kebijakan 4168
Dokumen kebijakan JSON 4169
Pelajari selengkapnya 4175
TranslateFullAccess 4175
Menggunakan kebijakan ini 4175
Rincian kebijakan 4175
Versi kebijakan 4175
Dokumen kebijakan JSON 4175
Pelajari selengkapnya 4176
TranslateReadOnly 4176
Menggunakan kebijakan ini 4176
Rincian kebijakan 4176
Versi kebijakan 4177
Dokumen kebijakan JSON 4177
Pelajari selengkapnya 4177
ViewOnlyAccess 4178
Menggunakan kebijakan ini 4178
Rincian kebijakan 4178
Versi kebijakan 4178
Dokumen kebijakan JSON 4178
Pelajari selengkapnya 4187
VMImportExportRoleForAWSConnector 4187
Menggunakan kebijakan ini 4188
Rincian kebijakan 4188
Versi kebijakan 4188
Dokumen kebijakan JSON 4188
Pelajari selengkapnya 4189

VPCLatticeFullAccess 4189
Menggunakan kebijakan ini 4189
Rincian kebijakan 4189
Versi kebijakan 4190
Dokumen kebijakan JSON 4190
Pelajari selengkapnya 4192
VPCLatticeReadOnlyAccess 4192
Menggunakan kebijakan ini 4192
Rincian kebijakan 4192
Versi kebijakan 4192
Dokumen kebijakan JSON 4193
Pelajari selengkapnya 4193
VPCLatticeServicesInvokeAccess 4194
Menggunakan kebijakan ini 4194
Rincian kebijakan 4194
Versi kebijakan 4194
Dokumen kebijakan JSON 4194
Pelajari selengkapnya 4195
WAFLoggingServiceRolePolicy 4195
Menggunakan kebijakan ini 4195
Rincian kebijakan 4195
Versi kebijakan 4195
Dokumen kebijakan JSON 4196
Pelajari selengkapnya 4196
WAFRegionalLoggingServiceRolePolicy 4196
Menggunakan kebijakan ini 4196
Rincian kebijakan 4196
Versi kebijakan 4197
Dokumen kebijakan JSON 4197
Pelajari selengkapnya 4197
WAFV2LoggingServiceRolePolicy 4197
Menggunakan kebijakan ini 4198
Rincian kebijakan 4198
Versi kebijakan 4198
Dokumen kebijakan JSON 4198
Pelajari selengkapnya 4199

WellArchitectedConsoleFullAccess 4199
Menggunakan kebijakan ini 4199
Rincian kebijakan 4199
Versi kebijakan 4199
Dokumen kebijakan JSON 4200
Pelajari selengkapnya 4200
WellArchitectedConsoleReadOnlyAccess 4200
Menggunakan kebijakan ini 4200
Rincian kebijakan 4201
Versi kebijakan 4201
Dokumen kebijakan JSON 4201
Pelajari selengkapnya 4201
WorkLinkServiceRolePolicy 4202
Menggunakan kebijakan ini 4202
Rincian kebijakan 4202
Versi kebijakan 4202
Dokumen kebijakan JSON 4202
Pelajari selengkapnya 4203
..... mmmmcciv

Apa itu kebijakan yang AWS dikelola?

Kebijakan AWS terkelola adalah kebijakan mandiri yang dibuat dan dikelola oleh AWS. AWS kebijakan terkelola dirancang untuk memberikan izin untuk banyak kasus penggunaan umum. Mereka memudahkan Anda untuk memulai dengan menetapkan izin kepada pengguna, grup, dan peran daripada jika Anda harus menulis kebijakan sendiri.

Perlu diingat bahwa kebijakan AWS terkelola mungkin tidak memberikan izin hak istimewa paling sedikit untuk kasus penggunaan spesifik Anda karena tersedia untuk digunakan oleh semua pelanggan. AWS Kami menyarankan Anda untuk mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola pelanggan yang khusus untuk kasus penggunaan Anda.

Anda tidak dapat mengubah izin yang ditentukan dalam kebijakan AWS terkelola. Jika AWS memperbarui izin yang ditentukan dalam kebijakan AWS terkelola, pembaruan akan memengaruhi semua identitas utama (pengguna, grup, dan peran) yang dilampirkan kebijakan tersebut. AWS kemungkinan besar akan memperbarui kebijakan AWS terkelola saat AWS layanan baru diluncurkan atau operasi API baru tersedia untuk layanan yang ada.

Untuk informasi selengkapnya, lihat kebijakan AWS terkelola di Panduan Pengguna IAM.

Memahami halaman referensi kebijakan

Setiap halaman referensi kebijakan mencakup informasi berikut:

- Menggunakan kebijakan ini — Apakah Anda dapat melampirkan kebijakan ke pengguna, grup, dan peran
- Rincian kebijakan
  - Jenis — Jenis kebijakan AWS terkelola
    - `AWS managed policy`— Kebijakan AWS terkelola standar
    - `Job function policy`— Kebijakan yang sejalan dengan fungsi pekerjaan industri umum
    - `Service-linked role policy`Kebijakan yang dilampirkan pada peran terkait layanan yang memungkinkan layanan untuk melakukan tindakan atas nama Anda, seperti the section called “AmazonRDSPreviewServiceRolePolicy”
    - `Service role policy`— Kebijakan yang dirancang untuk bekerja dengan peran layanan, seperti the section called “AWSControlTowerServiceRolePolicy”
  - Waktu pembuatan — Saat kebijakan pertama kali dibuat

  - Waktu yang diedit - Saat versi kebijakan ini diedit
  - ARN - Nama Sumber Daya Amazon dari kebijakan
- Versi kebijakan — Versi izin yang diberikan oleh kebijakan
- Dokumen kebijakan JSON — Kebijakan JSON
- Pelajari selengkapnya - Tautan ke dokumentasi yang terkait dengan kebijakan AWS terkelola

Kebijakan terkelola yang tidak digunakan lagi AWS

AWS memperbarui kebijakan AWS terkelola secara berkala. Dalam kebanyakan kasus, kami menambahkan izin ke kebijakan. Ini terjadi ketika kami meluncurkan layanan atau fitur baru. Untuk meningkatkan keamanan kebijakan yang AWS dikelola, terkadang kami mengurangi ruang lingkup kebijakan. Saat kami menghapus izin dari kebijakan, kami menetapkan kebijakan ke status usang dan membuat yang baru tersedia. Saat AWS menghentikan layanan atau fitur, kami juga menghentikan kebijakan terkelola untuk fitur tersebut. AWS

Jika Anda menerima pemberitahuan email bahwa kebijakan yang Anda gunakan tidak berlaku lagi, kami sarankan Anda segera mengambil tindakan. Identifikasi perubahan kebijakan dan perbarui alur kerja Anda. Jika AWS menyediakan kebijakan penggantian, rencanakan untuk melampirkannya ke semua identitas yang terpengaruh (pengguna, grup, dan peran), lalu lepaskan kebijakan yang tidak digunakan lagi dari identitas tersebut.

Kebijakan usang memiliki karakteristik sebagai berikut:

- Itu dihapus dari panduan ini.
- Izin terus berfungsi untuk semua identitas yang saat ini dilampirkan.
- Di akun tempat kebijakan dilampirkan ke identitas, muncul di daftar Kebijakan di konsol IAM dengan ikon peringatan di sebelahnya.
- Itu tidak dapat dilampirkan pada identitas baru apa pun. Jika Anda melepaskannya dari identitas saat ini, Anda tidak dapat memasangnya kembali.
- Setelah Anda melepaskannya dari semua entitas saat ini, itu tidak lagi terlihat.

AWS kebijakan terkelola

AWS kebijakan terkelola

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

- AmazonAugmentedAIHumanLoopFullAccess
- AmazonAugmentedAIIntegratedAPIAccess
- AmazonAuroraDSQLConsoleFullAccess
- AmazonAuroraDSQLFullAccess
- AmazonAuroraDSQLReadOnlyAccess
- AmazonBedrockFullAccess
- AmazonBedrockLimitedAccess
- 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
- AmazonEC2ReadOnlyAccess
- AmazonEC2RoleforAWSCodeDeploy
- AmazonEC2RoleforAWSCodeDeployLimited
- AmazonEC2RoleforDataPipelineRole
- AmazonEC2RoleforSSM
- AmazonEC2RolePolicyForLaunchWizard
- AmazonEC2SpotFleetAutoscaleRole
- AmazonEC2SpotFleetTaggingRole
- AmazonECS_FullAccess
- AmazonECSComputeServiceRolePolicy
- AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity
- AmazonECSInfrastructureRolePolicyForVolumes

- AmazonECSInfrastructureRolePolicyForVpcLattice
- AmazonECSServiceRolePolicy
- AmazonECSTaskExecutionRolePolicy
- AmazonEFSCSIDriverPolicy
- AmazonEKS_CNI_Policy
- AmazonEKSBlockStoragePolicy
- AmazonEKSClusterPolicy
- AmazonEKSComputePolicy
- AmazonEKSConnectorServiceRolePolicy
- AmazonEKSDashboardConsoleReadOnly
- AmazonEKSDashboardServiceRolePolicy
- AmazonEKSFargatePodExecutionRolePolicy
- AmazonEKSForFargateServiceRolePolicy
- AmazonEKSLoadBalancingPolicy
- AmazonEKSLocalOutpostClusterPolicy
- AmazonEKSLocalOutpostServiceRolePolicy
- 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
- 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
- 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
- AmazonSageMakerMechanicalTurkAccess
- AmazonSageMakerModelGovernanceUseAccess
- AmazonSageMakerModelRegistryFullAccess
- AmazonSageMakerNotebooksServiceRolePolicy
- AmazonSageMakerPartnerAppsFullAccess
- AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy
- AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy
- AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy
- AmazonSageMakerPipelinesIntegrations
- AmazonSageMakerQuickSightVPCPolicy
- AmazonSageMakerReadOnly
- AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy
- 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
- 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
- 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
- AWSBackupOperatorAccess
- AWSBackupOrganizationAdminAccess
- AWSBackupRestoreAccessForSAPHANA
- AWSBackupSearchOperatorAccess
- AWSBackupServiceLinkedRolePolicyForBackup
- AWSBackupServiceLinkedRolePolicyForBackupTest
- AWSBackupServiceRolePolicyForBackup

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

- AWSCleanRoomsReadOnlyAccess
- AWSCloud9Administrator
- AWSCloud9EnvironmentMember
- AWSCloud9ServiceRolePolicy
- AWSCloud9SSMInstanceProfile
- AWSCloud9User
- AWSCloudFormationFullAccess
- AWSCloudFormationReadOnlyAccess
- AWSCloudFrontLogger
- 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
- 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
- AWSDiscoveryContinuousExportFirehosePolicy
- AWSDMSFleetAdvisorServiceRolePolicy
- AWSDMSServerlessServiceRolePolicy
- AWSEC2CapacityReservationFleetRolePolicy
- AWSEC2FleetServiceRolePolicy
- AWSEC2SpotFleetServiceRolePolicy
- AWSEC2SpotServiceRolePolicy
- AWSEC2VssSnapshotPolicy
- AWSECRPullThroughCache_ServiceRolePolicy
- AWSElasticBeanstalkCustomPlatformforEC2Role
- AWSElasticBeanstalkEnhancedHealth
- AWSElasticBeanstalkMaintenance
- AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy
- AWSElasticBeanstalkManagedUpdatesServiceRolePolicy
- AWSElasticBeanstalkMulticontainerDocker
- AWSElasticBeanstalkReadOnly
- AWSElasticBeanstalkRoleCore
- AWSElasticBeanstalkRoleCWL
- AWSElasticBeanstalkRoleECS
- AWSElasticBeanstalkRoleRDS

- AWSElasticBeanstalkRoleSNS
- AWSElasticBeanstalkRoleWorkerTier
- AWSElasticBeanstalkService
- AWSElasticBeanstalkServiceRolePolicy
- AWSElasticBeanstalkWebTier
- AWSElasticBeanstalkWorkerTier
- AWSElasticDisasterRecoveryAgentInstallationPolicy
- AWSElasticDisasterRecoveryAgentPolicy
- AWSElasticDisasterRecoveryConsoleFullAccess
- AWSElasticDisasterRecoveryConsoleFullAccess_v2
- AWSElasticDisasterRecoveryConversionServerPolicy
- AWSElasticDisasterRecoveryCrossAccountReplicationPolicy
- AWSElasticDisasterRecoveryEc2InstancePolicy
- AWSElasticDisasterRecoveryFailbackInstallationPolicy
- AWSElasticDisasterRecoveryFailbackPolicy
- AWSElasticDisasterRecoveryLaunchActionsPolicy
- AWSElasticDisasterRecoveryNetworkReplicationPolicy
- AWSElasticDisasterRecoveryReadOnlyAccess
- AWSElasticDisasterRecoveryRecoveryInstancePolicy
- AWSElasticDisasterRecoveryReplicationServerPolicy
- AWSElasticDisasterRecoveryServiceRolePolicy
- AWSElasticDisasterRecoveryStagingAccountPolicy
- AWSElasticDisasterRecoveryStagingAccountPolicy_v2
- AWSElasticLoadBalancingClassicServiceRolePolicy
- AWSElasticLoadBalancingServiceRolePolicy
- 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
- 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
- AWSLambdaBasicExecutionRole
- AWSLambdaDynamoDBExecutionRole
- AWSLambdaENIManagementAccess
- AWSLambdaExecute
- AWSLambdaFullAccess
- AWSLambdaInvocation-DynamoDB
- AWSLambdaKinesisExecutionRole
- AWSLambdaMSKExecutionRole

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

- AWSMarketplaceSellerOfferManagement
- AWSMarketplaceSellerProductsFullAccess
- AWSMarketplaceSellerProductsReadOnly
- 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
- AWSNetworkFirewallFullAccess
- AWSNetworkFirewallReadOnlyAccess
- AWSNetworkFirewallServiceRolePolicy
- AWSNetworkManagerCloudWANServiceRolePolicy
- AWSNetworkManagerFullAccess
- AWSNetworkManagerReadOnlyAccess

- AWSNetworkManagerServiceRolePolicy
- AWSObservabilityAdminServiceRolePolicy
- AWSOpsWorks_FullAccess
- AWSOpsWorksCloudWatchLogs
- AWSOpsWorksCMInstanceProfileRole
- AWSOpsWorksCMServiceRole
- AWSOpsWorksInstanceRegistration
- AWSOpsWorksRegisterCLI_EC2
- AWSOpsWorksRegisterCLI_OnPremises
- AWSOrganizationsFullAccess
- AWSOrganizationsReadOnlyAccess
- AWSOrganizationsServiceTrustPolicy
- AWSOutpostsAuthorizeServerPolicy
- AWSOutpostsServiceRolePolicy
- AWSPanoramaApplianceRolePolicy
- AWSPanoramaApplianceServiceRolePolicy
- AWSPanoramaFullAccess
- AWSPanoramaGreengrassGroupRolePolicy
- AWSPanoramaSageMakerRolePolicy
- AWSPanoramaServiceLinkedRolePolicy
- AWSPanoramaServiceRolePolicy
- AWSPartnerCentralFullAccess
- 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
- 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
- AWSRolesAnywhereServicePolicy
- AWSS3OnOutpostsServiceRolePolicy
- AWSSavingsPlansFullAccess
- AWSSavingsPlansReadOnlyAccess
- 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
- AWSTrustedAdvisorPriorityFullAccess
- AWSTrustedAdvisorPriorityReadOnlyAccess
- AWSTrustedAdvisorReportingServiceRolePolicy
- AWSTrustedAdvisorServiceRolePolicy
- AWSUserNotificationsServiceLinkedRolePolicy
- AWSVendorInsightsAssessorFullAccess
- AWSVendorInsightsAssessorReadOnly
- AWSVendorInsightsVendorFullAccess
- AWSVendorInsightsVendorReadOnly
- AWSVpcLatticeServiceRolePolicy
- AWSVPCS2SVpnServiceRolePolicy
- AWSVPCTransitGatewayServiceRolePolicy
- AWSVPCVerifiedAccessServiceRolePolicy
- AWSWAFConsoleFullAccess
- AWSWAFConsoleReadOnlyAccess
- AWSWAFFullAccess
- AWSWAFReadOnlyAccess
- AWSWellArchitectedDiscoveryServiceRolePolicy
- AWSWellArchitectedOrganizationsServiceRolePolicy
- AWSWickrFullAccess
- AWSXrayCrossAccountSharingConfiguration
- AWSXRayDaemonWriteAccess

- AWSXrayFullAccess
- AWSXrayReadOnlyAccess
- AWSXrayWriteOnlyAccess
- AWSZonalAutoshiftPracticeRunSLRPolicy
- AWSZoneGroupAccessManagementServiceRolePolicy
- BatchServiceRolePolicy
- Billing
- 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
- ComputeOptimizerReadOnlyAccess

- ComputeOptimizerServiceRolePolicy
- ConfigConformsServiceRolePolicy
- CostOptimizationHubAdminAccess
- CostOptimizationHubReadOnlyAccess
- CostOptimizationHubServiceRolePolicy
- CustomerProfilesServiceLinkedRolePolicy
- DatabaseAdministrator
- DataScientist
- DAXServiceRolePolicy
- DeclarativePoliciesEC2Report
- DynamoDBCloudWatchContributorInsightsServiceRolePolicy
- DynamoDBKinesisReplicationServiceRolePolicy
- DynamoDBReplicationServiceRolePolicy
- EC2FastLaunchFullAccess
- EC2FastLaunchServiceRolePolicy
- EC2FleetTimeShiftableServiceRolePolicy
- Ec2ImageBuilderCrossAccountDistributionAccess
- EC2ImageBuilderLifecycleExecutionPolicy
- EC2InstanceConnect
- Ec2InstanceConnectEndpoint
- EC2InstanceProfileForImageBuilder
- EC2InstanceProfileForImageBuilderECRContainerBuilds
- ECRReplicationServiceRolePolicy
- ECRTemplateServiceRolePolicy
- ElastiCacheServiceRolePolicy
- ElasticLoadBalancingFullAccess
- ElasticLoadBalancingReadOnly
- ElementalActivationsDownloadSoftwareAccess
- ElementalActivationsFullAccess
- ElementalActivationsGenerateLicenses

- ElementalActivationsReadOnlyAccess
- ElementalAppliancesSoftwareFullAccess
- ElementalAppliancesSoftwareReadOnlyAccess
- ElementalSupportCenterFullAccess
- EMRDescribeClusterPolicyForEMRWAL
- FMSServiceRolePolicy
- FSxDeleteServiceLinkedRoleAccess
- 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
- 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
- ROSASRESupportPolicy
- ROSAWorkerInstancePolicy
- Route53RecoveryReadinessServiceRolePolicy
- Route53ResolverServiceRolePolicy
- S3StorageLensServiceRolePolicy
- SageMakerStudioAdminProjectUserRolePolicy
- SageMakerStudioBedrockAgentServiceRolePolicy
- SageMakerStudioBedrockChatAgentUserRolePolicy
- SageMakerStudioBedrockEvaluationJobServiceRolePolicy
- SageMakerStudioBedrockFlowServiceRolePolicy
- SageMakerStudioBedrockFunctionExecutionRolePolicy
- SageMakerStudioBedrockKnowledgeBaseCustomResourcePolicy
- SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy
- SageMakerStudioBedrockPromptUserRolePolicy
- SageMakerStudioDomainExecutionRolePolicy

- SageMakerStudioDomainServiceRolePolicy
- SageMakerStudioEMRInstanceRolePolicy
- SageMakerStudioEMRServiceRolePolicy
- SageMakerStudioFullAccess
- SageMakerStudioProjectProvisioningRolePolicy
- SageMakerStudioProjectRoleMachineLearningPolicy
- SageMakerStudioProjectUserRolePermissionsBoundary
- SageMakerStudioProjectUserRolePolicy
- SageMakerStudioQueryExecutionRolePolicy
- SecretsManagerReadWrite
- SecurityAudit
- SecurityLakeResourceManagementServiceRolePolicy
- SecurityLakeServiceLinkedRole
- ServerMigration_ServiceRole
- ServerMigrationConnector
- ServerMigrationServiceConsoleFullAccess
- ServerMigrationServiceLaunchRole
- ServerMigrationServiceRoleForInstanceValidation
- ServiceQuotasFullAccess
- ServiceQuotasReadOnlyAccess
- ServiceQuotasServiceRolePolicy
- SimpleWorkflowFullAccess
- SMSVoiceServiceRolePolicy
- SplitCostAllocationDataServiceRolePolicy
- SSMQuickSetupRolePolicy
- SupportUser
- SystemAdministrator
- TranslateFullAccess
- TranslateReadOnly
- ViewOnlyAccess

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

AccessAnalyzerServiceRolePolicy

Deskripsi: Izinkan Access Analyzer untuk menganalisis metadata sumber daya

`AccessAnalyzerServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 02 Desember 2019, 17:13 UTC
- Waktu yang telah diedit: 12 Mei 2025, 15:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AccessAnalyzerServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v17 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AccessAnalyzerServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:GetResourcePolicy",
        "dynamodb:ListStreams",
        "dynamodb:ListTables",
        "ec2:DescribeAddresses",
        "ec2:DescribeByoipCidrs",
        "ec2:DescribeSnapshotAttribute",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ec2:GetSnapshotBlockPublicAccessState",
        "ecr:DescribeRepositories",
        "ecr: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" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AdministratorAccess

Deskripsi: Menyediakan akses penuh ke AWS layanan dan sumber daya.

`AdministratorAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AdministratorAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:39 UTC
- Waktu telah diedit: 06 Februari 2015, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/AdministratorAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AdministratorAccess-Amplify

Deskripsi: Memberikan izin administratif akun sambil secara eksplisit mengizinkan akses langsung ke sumber daya yang dibutuhkan oleh aplikasi Amplify.

`AdministratorAccess-Amplify`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AdministratorAccess-Amplify` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Desember 2020, 19:03 UTC
- Waktu telah diedit: 04 April 2024, 20:35 UTC
- ARN: `arn:aws:iam::aws:policy/AdministratorAccess-Amplify`

Versi kebijakan

Versi kebijakan: v12 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CLICloudformationPolicy",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackEvents",
```

```
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:GetTemplate",
        "cloudformation:UpdateStack",
        "cloudformation:ListStacks",
        "cloudformation:ListStackResources",
        "cloudformation:DeleteStackSet",
        "cloudformation:DescribeStackSet",
        "cloudformation:UpdateStackSet",
        "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:*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AdministratorAccess-AWSElasticBeanstalk

Deskripsi: Memberikan izin administratif akun. Secara eksplisit memungkinkan pengembang dan administrator untuk mendapatkan akses langsung ke sumber daya yang mereka butuhkan untuk mengelola aplikasi Elastic AWS Beanstalk

`AdministratorAccess-AWSElasticBeanstalk`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AdministratorAccess-AWSElasticBeanstalk` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 22 Januari 2021 19:36 UTC
- Waktu yang telah diedit: 11 Desember 2024, 14:36 UTC
- ARN: `arn:aws:iam::aws:policy/AdministratorAccess-AWSElasticBeanstalk`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:Describe*",
        "acm:List*",
        "autoscaling:Describe*",
        "cloudformation:Describe*",
        "cloudformation:Estimate*",
        "cloudformation:Get*",
        "cloudformation:List*",
        "cloudformation:Validate*",
        "cloudtrail:LookupEvents",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "codecommit:Get*",
        "codecommit:UploadArchive",
        "ec2:AllocateAddress",
        "ec2:AssociateAddress",
        "ec2:AuthorizeSecurityGroup*",
        "ec2:CreateLaunchTemplate*",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags",
        "ec2:DeleteLaunchTemplate*",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteTags",
        "ec2:Describe*",
        "ec2:DisassociateAddress",
        "ec2:ReleaseAddress",
        "ec2:RevokeSecurityGroup*",
        "ecs:CreateCluster",
        "ecs:DeRegisterTaskDefinition",
        "ecs:Describe*",
        "ecs:List*",
        "ecs:RegisterTaskDefinition",
        "elasticbeanstalk:*",
        "elasticloadbalancing:Describe*",
        "iam:GetRole",
```

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

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

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

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

```
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AIOpsAssistantPolicy

Deskripsi: Memberikan ReadOnly izin yang diperlukan oleh Amazon AI Operations Assistant untuk melakukan analisis AWS sumber daya pelanggan selama penyelidikan.

`AIOpsAssistantPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AIOpsAssistantPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 02 Desember 2024, 16:21 UTC
- Waktu telah diedit: 03 April 2025, 22:22 UTC
- ARN: `arn:aws:iam::aws:policy/AIOpsAssistantPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "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: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: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: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:List*",
        "kinesisanalytics:Describe*",
        "kinesisanalytics:List*",
        "kinesisvideo:Describe*",
        "kms:DescribeKey",
        "kms:ListResourceTags",
        "kms:ListKeys",
        "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: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*",
        "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: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: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/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AIOpsConsoleAdminPolicy

Deskripsi: Memberikan akses penuh ke layanan Amazon AI Operations dan izin yang diperlukan melalui AWS konsol. Ini juga mencakup izin untuk menggunakan sesi konsol sadar identitas.

`AIOpsConsoleAdminPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AIOpsConsoleAdminPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 02 Desember 2024, 23:51 UTC
- Waktu yang telah diedit: 24 Juni 2025, 00:52 UTC
- ARN: `arn:aws:iam::aws:policy/AIOpsConsoleAdminPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AIOpsOperatorAccess

Deskripsi: Memberikan akses ke Operasi AI Amazon APIs untuk membuat, memperbarui, dan menghapus investigasi, peristiwa investigasi, dan sumber daya investigasi. Ini juga mencakup ReadOnly akses ke semua Operasi AI APIs dan untuk menggunakan sesi sadar identitas.

`AIOpsOperatorAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AIOpsOperatorAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 02 Desember 2024, 23:51 UTC
- Waktu yang telah diedit: 24 Juni 2025, 00:52 UTC
- ARN: `arn:aws:iam::aws:policy/AIOpsOperatorAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AIOpsReadOnlyAccess

Deskripsi: Memberikan ReadOnly izin ke layanan Amazon AI Operations dan sumber daya yang diperlukan.

`AIOpsReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AIOpsReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 02 Desember 2024, 23:51 UTC
- Waktu yang telah diedit: 24 Juni 2025, 00:22 UTC
- ARN: `arn:aws:iam::aws:policy/AIOpsReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AlexaForBusinessDeviceSetup

Deskripsi: Menyediakan akses pengaturan perangkat ke AlexaForBusiness layanan

`AlexaForBusinessDeviceSetup`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AlexaForBusinessDeviceSetup` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 November 2017, 16:47 UTC
- Waktu yang telah diedit: 20 Mei 2019, 21:05 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessDeviceSetup`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:RegisterDevice",
        "a4b:CompleteRegistration",
        "a4b:SearchDevices",
```

```
        "a4b:SearchNetworkProfiles",
        "a4b:GetNetworkProfile",
        "a4b:PutDeviceSetupEvents"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "A4bDeviceSetupAccess",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:A4BNetworkProfile*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AlexaForBusinessFullAccess

Deskripsi: Memberikan akses penuh ke AlexaForBusiness sumber daya dan akses ke terkait Layanan AWS

`AlexaForBusinessFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AlexaForBusinessFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 November 2017, 16:47 UTC

- Waktu yang telah diedit: 01 Juli 2020, 21:01 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessFullAccess`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:*",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : [
            "*a4b.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/*a4b.amazonaws.com/
AWSServiceRoleForAlexaForBusiness*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DeleteSecret",
        "secretsmanager:UpdateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:A4B*"
    },
    {
      "Effect" : "Allow",
      "Action" : "secretsmanager:CreateSecret",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:Name" : "A4B*"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AlexaForBusinessGatewayExecution

Deskripsi: Menyediakan akses eksekusi gateway ke AlexaForBusiness layanan

`AlexaForBusinessGatewayExecution`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AlexaForBusinessGatewayExecution` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 November 2017, 16:47 UTC
- Waktu telah diedit: 30 November 2017, 16:47 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessGatewayExecution`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
        "arn:aws:sqs:*:*:dd-*",
        "arn:aws:sqs:*:*:sd-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:List*",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogGroups",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AlexaForBusinessLifesizeDelegatedAccessPolicy

Deskripsi: Menyediakan akses ke perangkat Lifesize AVS

`AlexaForBusinessLifesizeDelegatedAccessPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AlexaForBusinessLifesizeDelegatedAccessPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 04 Juni 2020, 19:46 UTC

- Waktu yang telah diedit: 12 Juni 2020, 20:31 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessLifesizeDelegatedAccessPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AlexaForBusinessNetworkProfileServicePolicy

Deskripsi: Kebijakan ini memungkinkan Alexa for Business untuk melakukan tugas otomatis yang dijadwalkan oleh profil jaringan Anda.

`AlexaForBusinessNetworkProfileServicePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 13 Maret 2019, 00:53 UTC
- Waktu yang telah diedit: 05 April 2019, 21:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AlexaForBusinessNetworkProfileServicePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AlexaForBusinessPolyDelegatedAccessPolicy

Deskripsi: Menyediakan akses ke perangkat Poly AVS

`AlexaForBusinessPolyDelegatedAccessPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AlexaForBusinessPolyDelegatedAccessPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 16 Oktober 2019, 19:48 UTC
- Waktu yang telah diedit: 16 Oktober 2019, 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessPolyDelegatedAccessPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AlexaForBusinessReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke AlexaForBusiness layanan

`AlexaForBusinessReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AlexaForBusinessReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 November 2017, 16:47 UTC
- Waktu yang telah diedit: 20 November 2019, 00:25 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonAPIGatewayAdministrator

Deskripsi: Menyediakan akses penuh ke create/edit/delete APIs Amazon API Gateway melalui file AWS Management Console.

`AmazonAPIGatewayAdministrator`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonAPIGatewayAdministrator` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 09 Juli 2015, 17:34 UTC
- Waktu telah diedit: 09 Juli 2015, 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAPIGatewayAdministrator`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonAPIGatewayInvokeFullAccess

Deskripsi: Menyediakan akses penuh untuk memanggil APIs di Amazon API Gateway.

`AmazonAPIGatewayInvokeFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonAPIGatewayInvokeFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 09 Juli 2015, 17:36 UTC

- Waktu yang telah diedit: 18 Desember 2018, 18:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAPIGatewayInvokeFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonAPIGatewayPushToCloudWatchLogs

Deskripsi: Memungkinkan API Gateway untuk mendorong log ke akun pengguna.

`AmazonAPIGatewayPushToCloudWatchLogs`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonAPIGatewayPushToCloudWatchLogs` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 11 November 2015, 23:41 UTC
- Waktu telah diedit: 11 November 2015, 23:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonAPIGatewayPushToCloudWatchLogs`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonAppFlowFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon AppFlow dan akses ke AWS layanan yang didukung sebagai sumber aliran atau tujuan (S3 dan Redshift). Juga menyediakan akses ke KMS untuk enkripsi

`AmazonAppFlowFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonAppFlowFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 02 Juni 2020, 23:30 UTC
- Waktu telah diedit: 28 Februari 2022, 23.11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAppFlowFullAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "appflow:*",
      "Resource" : "*"
    },
    {
      "Sid" : "ListRolesForRedshift",
      "Effect" : "Allow",
      "Action" : "iam:ListRoles",
      "Resource" : "*"
    },
    {
      "Sid" : "KMSListAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSGrantAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "appflow.*.amazonaws.com"
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
```

```
        }
      }
    },
    {
      "Sid" : "KMSListGrantAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListGrants"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "appflow.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "S3ReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:GetBucketPolicy"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3PutBucketPolicyAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketPolicy"
      ],
      "Resource" : "arn:aws:s3:::appflow-*"
    },
    {
      "Sid" : "SecretsManagerCreateSecretAccess",
      "Effect" : "Allow",
      "Action" : "secretsmanager:CreateSecret",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:Name" : "appflow!*"
        },
```

```
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "appflow.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "SecretsManagerPutResourcePolicyAccess",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:PutResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "appflow.amazonaws.com"
          ]
        },
        "StringEqualsIgnoreCase" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "appflow"
        }
      }
    },
    {
      "Sid" : "LambdaListFunctions",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonAppFlowReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke aliran Amazon Appflow

`AmazonAppFlowReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonAppFlowReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 02 Juni 2020, 23:26 UTC
- Waktu telah diedit: 28 Februari 2022, 20.42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAppFlowReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appflow:DescribeConnector",
        "appflow:DescribeConnectors",
        "appflow:DescribeConnectorProfiles",
        "appflow:DescribeFlows",
        "appflow:DescribeFlowExecution",
```

```
        "appflow:DescribeConnectorFields",
        "appflow:ListConnectors",
        "appflow:ListConnectorFields",
        "appflow:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonAppStreamFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon AppStream melalui AWS Management Console.

`AmazonAppStreamFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonAppStreamFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu yang telah diedit: 28 Agustus 2020, 17:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAppStreamFullAccess`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "appstream:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget",
        "application-autoscaling:DescribeScheduledActions",
        "application-autoscaling:PutScheduledAction",
        "application-autoscaling:DeleteScheduledAction"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:PutMetricAlarm"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "ec2:DescribeRouteTables",
```

```
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : "iam:ListRoles",
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : "iam:PassRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/service-role/
ApplicationAutoScalingForAmazonAppStreamAccess",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "application-autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/appstream.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_AppStreamFleet",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "appstream.application-autoscaling.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonAppStreamPCAAccess

Deskripsi: Akses Amazon AppStream 2.0 ke AWS Certificate Manager Private CA di akun pelanggan untuk otentikasi berbasis sertifikat

`AmazonAppStreamPCAAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonAppStreamPCAAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 24 Oktober 2022, 17:05 UTC
- Waktu yang telah diedit: 24 Oktober 2022, 17.05 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonAppStreamPCAAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      "Action" : [
        "acm-pca:IssueCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:DescribeCertificateAuthority"
      ],
      "Resource" : "arn:*:acm-pca:*:*:*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/euc-private-ca" : "*"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonAppStreamReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon AppStream melalui AWS Management Console.

`AmazonAppStreamReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonAppStreamReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu telah diedit: 07 Desember 2016, 21:00 UTC

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

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonAppStreamServiceAccess

Deskripsi: Kebijakan default untuk peran AppStream layanan Amazon.

`AmazonAppStreamServiceAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonAppStreamServiceAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 19 November 2016, 04:17 UTC
- Waktu yang telah diedit: 26 Juni 2020, 16:33 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonAppStreamServiceAccess`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeAvailabilityZones",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeSubnets",
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcEndpoints",
        "s3:ListAllMyBuckets",
```

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonAthenaFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Athena dan akses cakupan ke dependensi yang diperlukan untuk mengaktifkan kueri, menulis hasil, dan manajemen data.

`AmazonAthenaFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonAthenaFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 November 2016, 16:46 UTC
- Waktu telah diedit: 03 Januari 2025, 00:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAthenaFullAccess`

Versi kebijakan

Versi kebijakan: v13 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonAugmentedAIFullAccess

Deskripsi: Menyediakan akses untuk melakukan semua operasi sumber daya Amazon Augmented AI, FlowDefinitions termasuk HumanTaskUis , HumanLoops dan. Tidak mengizinkan akses untuk membuat FlowDefinitions terhadap tim kerja kerumunan publik.

`AmazonAugmentedAIFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonAugmentedAIFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 Desember 2019, 16:21 UTC
- Waktu diedit: 03 Desember 2019, 16:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAugmentedAIFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonAugmentedAIHumanLoopFullAccess

Deskripsi: Menyediakan akses untuk melakukan semua operasi pada HumanLoops.

`AmazonAugmentedAIHumanLoopFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonAugmentedAIHumanLoopFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 Desember 2019, 16:20 UTC
- Waktu yang telah diedit: 03 Desember 2019, 16:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAugmentedAIHumanLoopFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonAugmentedAIIntegratedAPIAccess

Deskripsi: Menyediakan akses untuk melakukan semua operasi sumber daya Amazon Augmented AI, FlowDefinitions termasuk HumanTaskUis , HumanLoops dan. Juga menyediakan akses ke operasi layanan yang terintegrasi dengan Amazon Augmented AI.

`AmazonAugmentedAIIntegratedAPIAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonAugmentedAIIntegratedAPIAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 22 April 2020, 20:47 UTC
- Waktu yang telah diedit: 22 April 2020, 20:47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAugmentedAIIntegratedAPIAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonAuroraDSQLConsoleFullAccess

Deskripsi: Menyediakan konsol akses administratif penuh ke Aurora DSQL

`AmazonAuroraDSQLConsoleFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonAuroraDSQLConsoleFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 Desember 2024, 15:36 UTC
- Waktu yang telah diedit: 21 Mei 2025, 21:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAuroraDSQLConsoleFullAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      "Effect" : "Allow",
      "Action" : [
        "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"
        }
      }
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonAuroraDSQLFullAccess

Deskripsi: Menyediakan akses administratif penuh ke Aurora DSQL

`AmazonAuroraDSQLFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonAuroraDSQLFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 Desember 2024, 15:36 UTC
- Waktu yang telah diedit: 21 Mei 2025, 21:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAuroraDSQLFullAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonAuroraDSQLReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Aurora DSQL

`AmazonAuroraDSQLReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonAuroraDSQLReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 Desember 2024, 15:21 UTC
- Waktu yang telah diedit: 14 Mei 2025, 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAuroraDSQLReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonBedrockFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Bedrock serta akses terbatas ke layanan terkait yang diperlukan olehnya

`AmazonBedrockFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonBedrockFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Desember 2023, 15:47 UTC
- Waktu telah diedit: 29 Juni 2025, 22:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockFullAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
    {
      "Sid" : "APIsWithAllResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "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"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonBedrockLimitedAccess

Deskripsi: Menyediakan akses terbatas ke Amazon Bedrock serta layanan terkait yang diperlukan olehnya

`AmazonBedrockLimitedAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonBedrockLimitedAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 Juni 2025, 22:22 UTC
- Waktu telah diedit: 29 Juni 2025, 22:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockLimitedAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "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" : "MarketplaceOperationsFromBedrockFor3pModels",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:Subscribe",
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:Unsubscribe"
      ],
```

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonBedrockMarketplaceAccess

Deskripsi: Menyediakan akses terbatas ke Amazon Bedrock Marketplace serta layanan terkait yang diperlukan olehnya

`AmazonBedrockMarketplaceAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonBedrockMarketplaceAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 Juni 2025, 22:22 UTC
- Waktu telah diedit: 29 Juni 2025, 22:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockMarketplaceAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonBedrockReadOnly

Deskripsi: Menyediakan akses baca saja ke Amazon Bedrock

`AmazonBedrockReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonBedrockReadOnly` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 06 Desember 2023, 15:48 UTC
- Waktu telah diedit: 04 Desember 2024, 19:36 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockReadOnly`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonBedrockStudioPermissionsBoundary

Deskripsi: Mendefinisikan izin maksimum peran IAM yang dibuat Amazon Bedrock Studio untuk mengoperasikan sumber daya Amazon Bedrock Studio.

`AmazonBedrockStudioPermissionsBoundary`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonBedrockStudioPermissionsBoundary` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Agustus 2024, 00:24 UTC
- Waktu yang telah diedit: Agustus 01, 2024, 00:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockStudioPermissionsBoundary`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonBraketFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Braket melalui AWS Management Console dan SDK. Juga menyediakan akses ke layanan terkait (misalnya, S3, log).

`AmazonBraketFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonBraketFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Agustus 2020, 20:12 UTC
- Waktu telah diedit: 11 April 2025, 22:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBraketFullAccess`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonBraketJobsExecutionPolicy

Deskripsi: Memberikan akses Layanan AWS dan sumber daya yang diperlukan untuk menjalankan Pekerjaan Amazon Braket termasuk S3, Cloudwatch, IAM, dan Braket

`AmazonBraketJobsExecutionPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonBraketJobsExecutionPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 26 November 2021 19:34 UTC
- Waktu telah diedit: 28 November 2021, 05:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBraketJobsExecutionPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
        "s3:PutBucketPolicy"
      ],
      "Resource" : "arn:aws:s3:::amazon-braket-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "ecr:BatchCheckLayerAvailability"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/amazon-braket*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "braket:CancelJob",
        "braket:CancelQuantumTask",
        "braket:CreateJob",
        "braket:CreateQuantumTask",
        "braket:GetDevice",
        "braket:GetJob",
        "braket:GetQuantumTask",
        "braket:SearchDevices",
        "braket:SearchJobs",
        "braket:SearchQuantumTasks",
        "braket:ListTagsForResource",
        "braket:TagResource",
        "braket:UntagResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
```

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

```
          "cloudwatch:namespace" : "/aws/braket"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonBraketServiceRolePolicy

Deskripsi: Memungkinkan Amazon Braket untuk membuat dan mengelola AWS sumber daya atas nama Anda

`AmazonBraketServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 04 Agustus 2020, 17:12 UTC
- Waktu yang telah diedit: 06 Agustus 2020, 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonBraketServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonChimeFullAccess

Deskripsi: Menyediakan akses penuh ke Konsol Admin Amazon Chime melalui. AWS Management Console

`AmazonChimeFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonChimeFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 November 2017, 22:15 UTC
- Waktu yang telah diedit: 14 Desember 2020, 21:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonChimeFullAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

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

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonChimeReadOnly

Deskripsi: Menyediakan akses baca saja ke Konsol Admin Amazon Chime melalui. AWS Management Console

`AmazonChimeReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonChimeReadOnly` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 November 2017, 22:04 UTC
- Waktu yang telah diedit: 14 Desember 2020, 20:53 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonChimeReadOnly`

Versi kebijakan

Versi kebijakan: v10 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonChimeSDK

Deskripsi: Menyediakan akses ke operasi Amazon Chime SDK

`AmazonChimeSDK`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonChimeSDK` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 04 Februari 2020, 21:53 UTC
- Waktu telah diedit: 10 Januari 2023, 18:05 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonChimeSDK`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy

Deskripsi: Kebijakan Terkelola Untuk Peran Tertaut Layanan Amazon Chime SDK MediaPipelines

`AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 04 April 2022, 22:02 UTC
- Waktu telah diedit: 08 Desember 2023, 19:14 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonChimeSDKMessagingServiceRolePolicy

Deskripsi: Memungkinkan Amazon Chime SDK Messaging untuk mengakses AWS sumber daya dan mengaktifkan fungsionalitas pesan

`AmazonChimeSDKMessagingServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 03 Maret 2023, 01:43 UTC
- Waktu telah diedit: 03 Maret 2023, 01:43 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeSDKMessagingServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonChimeServiceRolePolicy

Deskripsi: Mengaktifkan akses ke AWS Sumber Daya yang digunakan atau dikelola oleh Amazon Chime

`AmazonChimeServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 30 September 2019, 22:25 UTC
- Waktu yang telah diedit: 30 September 2019, 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonChimeTranscriptionServiceLinkedRolePolicy

Deskripsi: Memungkinkan Amazon Chime mengakses Amazon Transcribe dan Amazon Transcribe Medical atas nama Anda

`AmazonChimeTranscriptionServiceLinkedRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan

- Waktu pembuatan: 04 Agustus 2021 21:47 UTC
- Waktu yang telah diedit: 04 Agustus 2021 21:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeTranscriptionServiceLinkedRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonChimeUserManagement

Deskripsi: Menyediakan akses manajemen pengguna ke Konsol Admin Amazon Chime melalui. AWS Management Console

`AmazonChimeUserManagement`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonChimeUserManagement` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 November 2017, 22:17 UTC
- Waktu yang telah diedit: 18 Februari 2020, 19:26 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonChimeUserManagement`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
        "chime:UpdateUserLicenses",
        "chime:ResetPersonalPIN",
        "chime:LogoutUser",
        "chime:ListDomains",
        "chime:GetDomain",
        "chime:ListDirectories",
        "chime: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" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonChimeVoiceConnectorServiceLinkedRolePolicy

Deskripsi: Kebijakan terkelola untuk Peran Tertaut Layanan untuk Amazon Chime VoiceConnector

`AmazonChimeVoiceConnectorServiceLinkedRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 30 September 2019, 22:16 UTC
- Waktu yang telah diedit: 14 April 2023, 21:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeVoiceConnectorServiceLinkedRolePolicy`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:GetDataEndpoint",
        "kinesisvideo:PutMedia",
        "kinesisvideo:UpdateDataRetention",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:CreateStream"
      ],
      "Resource" : [
        "arn:aws:kinesisvideo:*:*:stream/ChimeVoiceConnector-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:ListStreams"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "SNS:Publish"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:ChimeVoiceConnector-Streaming*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:SendMessage"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:ChimeVoiceConnector-Streaming*"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "polly:SynthesizeSpeech"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "chime:CreateMediaInsightsPipeline",
        "chime:GetMediaInsightsPipelineConfiguration"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonCloudDirectoryFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Cloud Directory Service.

`AmazonCloudDirectoryFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonCloudDirectoryFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 25 Februari 2017, 00:41 UTC
- Waktu yang telah diedit: 25 Februari 2017, 00:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudDirectoryFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonCloudDirectoryReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon Cloud Directory Service.

`AmazonCloudDirectoryReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonCloudDirectoryReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 Februari 2017, 23:42 UTC
- Waktu telah diedit: 28 Februari 2017, 23:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudDirectoryReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonCloudWatchEvidentlyFullAccess

Deskripsi: Menyediakan akses penuh hanya ke Amazon CloudWatch Terbukti. Juga menyediakan akses ke Amazon S3 terkait, Amazon SNS, CloudWatch Amazon, dan layanan terkait lainnya.

`AmazonCloudWatchEvidentlyFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonCloudWatchEvidentlyFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 November 2021 15:10 UTC
- Waktu yang telah diedit: 29 November 2021 15.10 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchEvidentlyFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "evidently:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/CloudWatchRUMEvidentlyRole-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:TagResource",
        "cloudwatch:UnTagResource"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:LookupEvents"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:Evidently-Alarm-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : [
        "*"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:Subscribe",
        "sns:ListSubscriptionsByTopic"
      ],
      "Resource" : [
        "arn:*:sns:*:*:Evidently-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonCloudWatchEvidentlyReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke CloudWatch Amazon

`AmazonCloudWatchEvidentlyReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonCloudWatchEvidentlyReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 November 2021, 15:08 UTC
- Waktu yang telah diedit: 29 November 2021, 15:08 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchEvidentlyReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonCloudWatchEvidentlyServiceRolePolicy

Deskripsi: Memungkinkan Layanan CloudWatch Terbukti untuk mengelola AWS Sumber Daya terkait atas nama pelanggan

`AmazonCloudWatchEvidentlyServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 13 September 2022, 17:25 UTC
- Waktu yang telah diedit: 13 September 2022, 17.25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCloudWatchEvidentlyServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

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

```
          "aws:ResourceTag/DeployedBy" : "Evidently"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "appconfig:ListDeployments",
      "Resource" : "arn:aws:appconfig:*:*:application/*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonCloudWatchRUMFullAccess

Deskripsi: Memberikan izin akses penuh untuk layanan Amazon CloudWatch RUM

`AmazonCloudWatchRUMFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonCloudWatchRUMFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 November 2021 15:46 UTC
- Waktu yang telah diedit: 29 November 2021 15.46 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchRUMFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "rum:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/rum.amazonaws.com/
AWSServiceRoleForRealUserMonitoring"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/RUM-Monitor*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "cognito-identity.amazonaws.com"
          ]
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cognito-identity:CreateIdentityPool",
        "cognito-identity:ListIdentityPools",
        "cognito-identity:DescribeIdentityPool",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:SetIdentityPoolRoles"
      ],
      "Resource" : "arn:aws:cognito-identity:*:*:identitypool/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:DeleteLogGroup",
        "logs:PutRetentionPolicy",
        "logs:CreateLogStream"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:*RUMService*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
```

```
        "logs:ListLogDeliveries",
        "logs:DescribeResourcePolicies"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group::log-stream:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "synthetics:describeCanaries",
        "synthetics:describeCanariesLastRun"
      ],
      "Resource" : "arn:aws:synthetics:*:*:canary:*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonCloudWatchRUMReadOnlyAccess

Deskripsi: Memberikan izin baca saja untuk layanan Amazon CloudWatch RUM

`AmazonCloudWatchRUMReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonCloudWatchRUMReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 November 2021 15:43 UTC
- Waktu yang telah diedit: 12 Juni 2025, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchRUMReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonCloudWatchRUMServiceRolePolicy

Deskripsi: Memberikan izin kepada Amazon CloudWatch RUM Service untuk mempublikasikan data pemantauan ke layanan terkait AWS lainnya

`AmazonCloudWatchRUMServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 17 November 2021 23:17 UTC
- Waktu telah diedit: 22 Februari 2023, 20:35 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCloudWatchRUMServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonCodeCatalystFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon CodeCatalyst

`AmazonCodeCatalystFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonCodeCatalystFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 20 April 2023, 16:50 UTC
- Waktu telah diedit: April 20, 2023, 16:50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeCatalystFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CodeCatalystResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "codecatalyst:*",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeCatalystAssociateIAMRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "codecatalyst.amazonaws.com",
            "codecatalyst-runner.amazonaws.com"
          ]
        }
      }
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonCodeCatalystReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon CodeCatalyst

`AmazonCodeCatalystReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonCodeCatalystReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 20 April 2023, 16:49 UTC
- Waktu telah diedit: April 20, 2023, 16:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeCatalystReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonCodeCatalystSupportAccess

Deskripsi: CodeCatalyst Memungkinkan Amazon membuat, memperbarui, dan menyelesaikan AWS Dukungan kasus atas nama Anda.

`AmazonCodeCatalystSupportAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonCodeCatalystSupportAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 20 April 2023, 12:34 UTC

- Waktu telah diedit: April 20, 2023, 12:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonCodeCatalystSupportAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "support:DescribeAttachment",
        "support:DescribeCaseAttributes",
        "support:DescribeCases",
        "support:DescribeCommunications",
        "support:DescribeIssueTypes",
        "support:DescribeServices",
        "support:DescribeSeverityLevels",
        "support:DescribeSupportLevel",
        "support:SearchForCases",
        "support:AddAttachmentsToSet",
        "support:AddCommunicationToCase",
        "support:CreateCase",
        "support:InitiateCallForCase",
        "support:InitiateChatForCase",
        "support:PutCaseAttributes",
        "support:RateCaseCommunication",
        "support:ResolveCase"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonCodeGuruProfilerAgentAccess

Deskripsi: Menyediakan akses yang diperlukan oleh agen Amazon CodeGuru Profiler.

`AmazonCodeGuruProfilerAgentAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonCodeGuruProfilerAgentAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 05 Februari 2021 22:11 UTC
- Waktu yang telah diedit: 05 Mei 2022, 18.11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruProfilerAgentAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonCodeGuruProfilerFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon CodeGuru Profiler.

`AmazonCodeGuruProfilerFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonCodeGuruProfilerFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 Desember 2019, 10:13 UTC
- Waktu yang telah diedit: 15 Juli 2020, 03:23 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruProfilerFullAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codeguru-profiler:*",
        "iam:ListRoles",
        "iam:ListUsers",
        "sns:ListTopics",
        "codeguru:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/*AWSServiceRoleForCodeGuruProfiler*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "codeguru-profiler.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonCodeGuruProfilerReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon CodeGuru Profiler.

`AmazonCodeGuruProfilerReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonCodeGuruProfilerReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 Desember 2019, 10:30 UTC
- Waktu yang telah diedit: 27 Juni 2020, 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruProfilerReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
        "codeguru-profiler:BatchGet*",
        "codeguru-profiler:Describe*",
        "codeguru-profiler:Get*",
        "codeguru-profiler:List*",
        "iam:ListRoles",
        "iam:ListUsers"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonCodeGuruReviewerFullAccess

Deskripsi: Memberikan akses penuh ke Amazon CodeGuru Reviewer dan akses terbatas ke dependensi yang diperlukan.

`AmazonCodeGuruReviewerFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonCodeGuruReviewerFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 Desember 2019, 08:33 UTC
- Waktu telah diedit: 29 Agustus 2020, 04:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruReviewerFullAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonCodeGuruReviewerFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-reviewer:*",
        "codeguru:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonCodeGuruReviewerSLRCreation",
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/codeguru-
reviewer.amazonaws.com/AWSServiceRoleForAmazonCodeGuruReviewer",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "codeguru-reviewer.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonCodeGuruReviewerSLRDeletion",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/codeguru-
reviewer.amazonaws.com/AWSServiceRoleForAmazonCodeGuruReviewer"
```

```
    },
    {
      "Sid" : "CodeCommitAccess",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:ListRepositories"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeCommitTagManagement",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:TagResource",
        "codecommit:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "codeguru-reviewer"
        }
      }
    },
    {
      "Sid" : "CodeConnectTagManagement",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:TagResource",
        "codestar-connections:UntagResource",
        "codestar-connections:ListTagsForResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "codeguru-reviewer"
        }
      }
    },
    {
      "Sid" : "CodeConnectManagedRules",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection",
        "codestar-connections:ListConnections",
```

```
        "codestar-connections:PassConnection"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "codestar-connections:ProviderAction" : [
            "ListRepositories",
            "ListOwners"
          ]
        }
      }
    },
    {
      "Sid" : "CloudWatchEventsManagedRules",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:DeleteRule",
        "events:RemoveTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "codeguru-reviewer.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonCodeGuruReviewerReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon CodeGuru Reviewer.

`AmazonCodeGuruReviewerReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonCodeGuruReviewerReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 Desember 2019, 08:48 UTC
- Waktu telah diedit: 29 Agustus 2020, 04:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruReviewerReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonCodeGuruReviewerServiceRolePolicy

Deskripsi: Peran terkait layanan yang diperlukan untuk Amazon CodeGuru Reviewer untuk mengakses sumber daya atas nama Anda.

`AmazonCodeGuruReviewerServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 03 Desember 2019, 05:31 UTC
- Waktu yang telah diedit: 27 November 2020, 15:09 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCodeGuruReviewerServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonCodeGuruSecurityFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon CodeGuru Security.

`AmazonCodeGuruSecurityFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonCodeGuruSecurityFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 09 Mei 2023, 21:03 UTC
- Waktu yang telah diedit: 09 Mei 2023, 21:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruSecurityFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      "Effect" : "Allow",
      "Action" : [
        "codeguru-security:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonCodeGuruSecurityScanAccess

Deskripsi: Menyediakan akses yang diperlukan untuk bekerja dengan pemindaian Amazon CodeGuru Security.

`AmazonCodeGuruSecurityScanAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonCodeGuruSecurityScanAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 09 Mei 2023, 20:54 UTC
- Waktu yang telah diedit: 09 Mei 2023, 20:54 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruSecurityScanAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonCognitoDeveloperAuthenticatedIdentities

Deskripsi: Menyediakan akses ke Amazon Cognito APIs untuk mendukung identitas otentikasi developer dari backend otentikasi Anda.

`AmazonCognitoDeveloperAuthenticatedIdentities`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonCognitoDeveloperAuthenticatedIdentities` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 24 Maret 2015, 17:22 UTC
- Waktu telah diedit: 24 Maret 2015, 17:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoDeveloperAuthenticatedIdentities`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonCognitoIdpEmailServiceRolePolicy

Deskripsi: Memungkinkan layanan Amazon Cognito User Pools menggunakan identitas SES Anda untuk pengiriman email

`AmazonCognitoIdpEmailServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 21 Maret 2019, 21:32 UTC
- Waktu diedit: 21 Maret 2019, 21:32 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCognitoIdpEmailServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonCognitoIdpServiceRolePolicy

Deskripsi: Mengaktifkan akses ke Layanan AWS dan Sumber Daya yang digunakan atau dikelola oleh Kumpulan Pengguna Amazon Cognito

`AmazonCognitoIdpServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 26 Juni 2020, 22:30 UTC
- Waktu yang telah diedit: 26 Juni 2020, 22:30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCognitoIdpServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonCognitoPowerUser

Deskripsi: Menyediakan akses administratif ke sumber daya Amazon Cognito yang ada. Anda akan memerlukan hak Akun AWS admin untuk membuat sumber daya Cognito baru.

`AmazonCognitoPowerUser`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonCognitoPowerUser` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 24 Maret 2015, 17:14 UTC
- Waktu telah diedit: 27 Februari 2025, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoPowerUser`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
        "iam:ListSAMLProviders",
        "iam:GetSAMLProvider",
        "kinesis:ListStreams",
        "lambda:GetPolicy",
        "lambda:ListFunctions",
        "sns:GetSMSSandboxAccountStatus",
        "sns:ListPlatformApplications",
        "ses:ListIdentities",
        "ses:GetIdentityVerificationAttributes",
        "mobiletargeting:GetApps",
        "acm:ListCertificates",
        "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*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonCognitoReadOnly

Deskripsi: Menyediakan akses baca saja ke sumber daya Amazon Cognito.

`AmazonCognitoReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonCognitoReadOnly` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 24 Maret 2015, 17:06 UTC
- Waktu yang telah diedit: 1 Agustus 2019, 19:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoReadOnly`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonCognitoUnAuthedIdentitiesSessionPolicy

Deskripsi: Kebijakan ini mendefinisikan kumpulan izin yang diizinkan untuk identitas yang tidak diautentikasi untuk Kumpulan Identitas Cognito. Kebijakan ini tidak dimaksudkan untuk digunakan sebagai kebijakan izin yang berdiri sendiri. Ini digunakan sebagai pagar pembatas terhadap kebijakan yang terlalu permisif yang dilampirkan untuk peran dalam kumpulan identitas. Jangan lampirkan kebijakan ini ke peran apa pun, karena Layanan Identitas Cognito akan secara otomatis menyertakannya sebagai kebijakan cakupan bawah saat membuat kredensitas. Hak istimewa untuk mengakses sementara AWS sumber daya lain melalui aliran yang ditingkatkan sekarang akan

ditentukan oleh persimpangan peran yang terkait dengan identitas pengguna yang tidak diautentikasi yang disediakan oleh layanan, dan hak istimewa yang diberikan dalam kebijakan terkelola ini yang dimiliki oleh Cognito.

`AmazonCognitoUnAuthedIdentitiesSessionPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonCognitoUnAuthedIdentitiesSessionPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 19 Juli 2023, 23:04 UTC
- Waktu telah diedit: November 01, 2024, 18:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoUnAuthedIdentitiesSessionPolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin dengan hak istimewa paling sedikit

AmazonCognitoUnauthenticatedIdentities

Deskripsi: Kebijakan ini mendefinisikan kumpulan izin yang diizinkan untuk identitas yang tidak diautentikasi untuk Kumpulan Identitas Cognito. Ini tidak perlu dilampirkan ke peran unauth Anda, karena Layanan Identitas Cognito akan secara otomatis memasukkannya sebagai kebijakan cakupan

bawah saat membuat kredensional. Hak istimewa untuk mengakses sementara AWS sumber daya lain melalui aliran yang ditingkatkan sekarang akan ditentukan oleh persimpangan peran yang terkait dengan identitas pengguna yang tidak diautentikasi yang disediakan oleh layanan, dan hak istimewa yang diberikan dalam kebijakan terkelola ini yang dimiliki oleh Cognito.

`AmazonCognitoUnauthenticatedIdentities`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonCognitoUnauthenticatedIdentities` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Februari 2023, 22:36 UTC
- Waktu telah diedit: 01 Februari 2023, 22:36 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoUnauthenticatedIdentities`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonConnect_FullAccess

Deskripsi: Tujuan kebijakan ini adalah untuk memberikan izin kepada pengguna AWS Connect yang diperlukan untuk menggunakan sumber daya Connect. Kebijakan ini menyediakan akses penuh ke sumber daya AWS Connect melalui Connect Console dan publik APIs

`AmazonConnect_FullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonConnect_FullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 20 November 2020, 19:54 UTC
- Waktu telah diedit: 07 Maret 2023, 14:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonConnect_FullAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "connect:*",
        "ds:CreateAlias",
        "ds:AuthorizeApplication",
        "ds:CreateIdentityPoolDirectory",
        "ds:DeleteDirectory",
        "ds:DescribeDirectories",
        "ds:UnauthorizeApplication",
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams",
        "kinesis:DescribeStream",
        "kinesis:ListStreams",
        "kms:DescribeKey",
        "kms:ListAliases",
        "lex:GetBots",
        "lex:ListBots",
        "lex:ListBotAliases",
        "logs:CreateLogGroup",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "lambda:ListFunctions",
        "ds:CheckAlias",
        "profile:ListAccountIntegrations",
        "profile:GetDomain",
        "profile:ListDomains",
        "profile:GetProfileObjectType",
        "profile:ListProfileObjectTypeTemplates"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "profile:AddProfileKey",
        "profile:CreateDomain",
        "profile:CreateProfile",
```

```
        "profile:DeleteDomain",
        "profile:DeleteIntegration",
        "profile:DeleteProfile",
        "profile:DeleteProfileKey",
        "profile:DeleteProfileObject",
        "profile:DeleteProfileObjectType",
        "profile:GetIntegration",
        "profile:GetMatches",
        "profile:GetProfileObjectType",
        "profile:ListIntegrations",
        "profile:ListProfileObjects",
        "profile:ListProfileObjectTypes",
        "profile:ListTagsForResource",
        "profile:MergeProfiles",
        "profile:PutIntegration",
        "profile:PutProfileObject",
        "profile:PutProfileObjectType",
        "profile:SearchProfiles",
        "profile:TagResource",
        "profile:UntagResource",
        "profile:UpdateDomain",
        "profile:UpdateProfile"
      ],
      "Resource" : "arn:aws:profile:*:*:domains/amazon-connect-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:GetBucketAcl"
      ],
      "Resource" : "arn:aws:s3:::amazon-connect-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : "arn:aws:servicequotas:*:*:connect/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
```

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonConnectCampaignsServiceLinkedRolePolicy

Deskripsi: Kebijakan untuk peran terkait layanan Amazon Connect Campaigns

`AmazonConnectCampaignsServiceLinkedRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 23 September 2021 20:54 UTC
- Waktu telah diedit: 03 Oktober 2024, 20:20 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonConnectCampaignsServiceLinkedRolePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonConnectReadOnlyAccess

Deskripsi: Memberikan izin untuk melihat instans Amazon Connect di instans Anda. Akun AWS

`AmazonConnectReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonConnectReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 17 Oktober 2018, 21:00 UTC

- Waktu yang telah diedit: 19 Juni 2024, 15:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonConnectReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonConnectServiceLinkedRolePolicy

Deskripsi: Memungkinkan Amazon Connect membuat dan mengelola AWS sumber daya atas nama Anda.

`AmazonConnectServiceLinkedRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 07 September 2018, 00:21 UTC
- Waktu yang telah diedit: 01 Juli 2025, 00:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonConnectServiceLinkedRolePolicy`

Versi kebijakan

Versi kebijakan: v26 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

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

```
      "Sid" : "AllowConnectLogGroupAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/connect/*:*"
      ]
    },
    {
      "Sid" : "AllowListLexBotAccess",
      "Effect" : "Allow",
      "Action" : [
        "lex:ListBots",
        "lex:ListBotAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCustomerProfilesForConnectDomain",
      "Effect" : "Allow",
      "Action" : [
        "profile:SearchProfiles",
        "profile:CreateProfile",
        "profile:UpdateProfile",
        "profile:AddProfileKey",
        "profile:ListProfileObjectTypes",
        "profile:ListCalculatedAttributeDefinitions",
        "profile:ListCalculatedAttributesForProfile",
        "profile:GetDomain",
        "profile:ListIntegrations",
        "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"
      ],
      "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"
      ],
      "Resource" : [
        "arn:aws:profile:*:*:domains/amazon-connect-*/object-types/*"
      ]
    },
    {
      "Sid" : "AllowListIntegrationForCustomerProfile",
      "Effect" : "Allow",
      "Action" : [
        "profile:ListAccountIntegrations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadForCustomerProfileObjectTemplates",
      "Effect" : "Allow",
      "Action" : [
        "profile:ListProfileObjectTypeTemplates",
        "profile:GetProfileObjectTypeTemplate"
      ],
      "Resource" : "arn:aws:profile:*:*:/templates*"
    },
    {
      "Sid" : "AllowWisdomForConnectEnabledTaggedResources",
      "Effect" : "Allow",
      "Action" : [
        "wisdom:CreateContent",
        "wisdom:DeleteContent",
        "wisdom:CreateKnowledgeBase",
        "wisdom:GetAssistant",
        "wisdom:GetKnowledgeBase",
        "wisdom:GetContent",
        "wisdom:GetRecommendations",
        "wisdom:GetSession",
```

```
        "wisdom:NotifyRecommendationsReceived",
        "wisdom:QueryAssistant",
        "wisdom:StartContentUpload",
        "wisdom:UpdateContent",
        "wisdom:UntagResource",
        "wisdom:TagResource",
        "wisdom:CreateSession",
        "wisdom:CreateQuickResponse",
        "wisdom:GetQuickResponse",
        "wisdom:SearchQuickResponses",
        "wisdom:StartImportJob",
        "wisdom:GetImportJob",
        "wisdom:ListImportJobs",
        "wisdom:ListQuickResponses",
        "wisdom:UpdateQuickResponse",
        "wisdom:DeleteQuickResponse",
        "wisdom:PutFeedback",
        "wisdom:ListContentAssociations",
        "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"
      ],
      "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" : "AllowMobileTargetingOperationsForConnect",
      "Effect" : "Allow",
      "Action" : "mobiletargeting:SendMessages",
      "Resource" : "arn:aws:mobiletargeting:*:*:apps/*",
      "Condition" : {
        "StringEquals" : {
```

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonConnectSynchronizationServiceRolePolicy

Deskripsi: Mengizinkan Amazon Connect menyinkronkan AWS sumber daya di seluruh wilayah atas nama Anda.

`AmazonConnectSynchronizationServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 27 Oktober 2023, 22:38 UTC
- Waktu telah diedit: 12 November 2024, 22:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonConnectSynchronizationServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowConnectActions",
      "Effect" : "Allow",
      "Action" : [
        "connect:Create*",
        "connect:Update*",
        "connect:Delete*",
        "connect:Describe*",
        "connect:List*",
        "connect:Search*",
        "connect:Associate*",
        "connect:Disassociate*",
        "connect:Get*",
        "connect:BatchGet*",
        "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"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonConnectVoiceIDFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Connect Voice ID

`AmazonConnectVoiceIDFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonConnectVoiceIDFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 26 September 2021 19:04 UTC
- Waktu yang telah diedit: 26 September 2021, 19:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonConnectVoiceIDFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonDataZoneBedrockModelConsumptionPolicy

Deskripsi: Menyediakan izin untuk menggunakan model Amazon Bedrock, termasuk memanggil profil inferensi aplikasi Amazon Bedrock yang dibuat untuk domain Amazon tertentu. DataZone

`AmazonDataZoneBedrockModelConsumptionPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDataZoneBedrockModelConsumptionPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 12 November 2024, 22:15 UTC
- Waktu yang telah diedit: 28 Mei 2025, 18:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneBedrockModelConsumptionPolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonDataZoneBedrockModelManagementPolicy

Deskripsi: Menyediakan izin untuk mengelola akses model Amazon Bedrock, termasuk membuat, menandai, dan menghapus profil inferensi aplikasi.

`AmazonDataZoneBedrockModelManagementPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDataZoneBedrockModelManagementPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 12 November 2024, 22:14 UTC
- Waktu telah diedit: 12 November 2024, 22:14 UTC

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

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonDataZoneDomainExecutionRolePolicy

Deskripsi: Kebijakan default untuk peran DomainExecutionRole layanan Amazon DataZone. Peran ini digunakan oleh Amazon DataZone untuk membuat katalog, menemukan, mengatur, berbagi, dan menganalisis data dalam DataZone domain Amazon.

`AmazonDataZoneDomainExecutionRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDataZoneDomainExecutionRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 27 September 2023, 21:55 UTC
- Waktu yang telah diedit: 03 Desember 2024, 14:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneDomainExecutionRolePolicy`

Versi kebijakan

Versi kebijakan: v10 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonDataZoneEnvironmentRolePermissionsBoundary

Deskripsi: Amazon DataZone membuat peran IAM untuk Lingkungan untuk melakukan tindakan analitik data, dan menggunakan kebijakan ini saat membuat peran ini untuk menentukan batas izinnya.

`AmazonDataZoneEnvironmentRolePermissionsBoundary`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDataZoneEnvironmentRolePermissionsBoundary` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 11 September 2023, 23:38 UTC
- Waktu telah diedit: 17 November 2023, 23:29 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneEnvironmentRolePermissionsBoundary`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
          ]
        }
      }
    },
    {
      "Sid" : "GlueOperations",
      "Effect" : "Allow",
      "Action" : [
        "glue:*DataQuality*",
        "glue:BatchCreatePartition",
        "glue:BatchDeleteConnection",
        "glue:BatchDeletePartition",
        "glue:BatchDeleteTable",
        "glue:BatchDeleteTableVersion",
        "glue:BatchGetJobs",
        "glue:BatchGetWorkflows",
        "glue:BatchStopJobRun",
        "glue:BatchUpdatePartition",
        "glue:CreateBlueprint",
        "glue:CreateConnection",
        "glue:CreateCrawler",
        "glue:CreateDatabase",
        "glue:CreateJob",
        "glue:CreatePartition",
        "glue:CreatePartitionIndex",
        "glue:CreateTable",
        "glue:CreateWorkflow",
        "glue:DeleteBlueprint",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeleteConnection",
        "glue:DeleteCrawler",
        "glue:DeleteJob",
        "glue:DeletePartition",
        "glue:DeletePartitionIndex",
        "glue:DeleteTable",
        "glue:DeleteTableVersion",
        "glue:DeleteWorkflow",
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:GetConnection",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
```

```
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:ListSchemas",
        "glue:ListJobs",
        "glue:NotifyEvent",
        "glue:PutWorkflowRunProperties",
        "glue:ResetJobBookmark",
        "glue:ResumeWorkflowRun",
        "glue:SearchTables",
        "glue:StartBlueprintRun",
        "glue:StartCrawler",
        "glue:StartCrawlerSchedule",
        "glue:StartJobRun",
        "glue:StartWorkflowRun",
        "glue:StopCrawler",
        "glue:StopCrawlerSchedule",
        "glue:StopWorkflowRun",
        "glue:UpdateBlueprint",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:UpdateConnection",
        "glue:UpdateCrawler",
        "glue:UpdateCrawlerSchedule",
        "glue:UpdateDatabase",
        "glue:UpdateJob",
        "glue:UpdatePartition",
        "glue:UpdateTable",
        "glue:UpdateWorkflow"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "PassRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
```

```
        "arn:aws:iam::*:role/datazone*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "glue.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SameAccountKmsOperations",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:Decrypt",
        "kms:ListKeys"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "KmsOperationsWithResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:Decrypt",
        "kms:ListKeys",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:Verify",
        "kms:Sign"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "AnalyticsOperations",
```

```
      "Effect" : "Allow",
      "Action" : [
        "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" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonDataZoneFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon DataZone melalui AWS Management Console serta akses terbatas ke layanan terkait yang diperlukan olehnya.

`AmazonDataZoneFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDataZoneFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 22 September 2023, 20:06 UTC
- Waktu yang telah diedit: 22 Mei 2025, 18:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneFullAccess`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonDataZoneStatement",
      "Effect" : "Allow",
      "Action" : [
        "datazone:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ReadOnlyStatement",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "iam:ListRoles",
        "sso:DescribeRegisteredRegions",
        "s3:ListAllMyBuckets",
        "redshift:DescribeClusters",
        "redshift-serverless:ListWorkgroups",
        "ec2: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"
        }
      }
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonDataZoneFullUserAccess

Deskripsi: Menyediakan akses penuh ke Amazon DataZone, tetapi tidak mengizinkan pengelolaan domain, pengguna, atau akun terkait.

`AmazonDataZoneFullUserAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDataZoneFullUserAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 22 September 2023, 21:06 UTC
- Waktu telah diedit: 19 November 2024, 21:38 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneFullUserAccess`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin dengan hak istimewa paling sedikit

AmazonDataZoneGlueManageAccessRolePolicy

Deskripsi: Kebijakan ini memberikan izin untuk mengizinkan Amazon mengaktifkan penerbitan dan akses hibah DataZone ke data.

`AmazonDataZoneGlueManageAccessRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDataZoneGlueManageAccessRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 22 September 2023, 20:21 UTC
- Waktu telah diedit: 19 Juni 2025, 19:37 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneGlueManageAccessRolePolicy`

Versi kebijakan

Versi kebijakan: v10 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "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}"
        }
```

```
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonDataZonePortalFullAccessPolicy

Deskripsi: Menyediakan akses penuh ke Amazon DataZone APIs

`AmazonDataZonePortalFullAccessPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDataZonePortalFullAccessPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 26 Maret 2023, 18:24 UTC
- Waktu telah diedit: 26 Maret 2023, 18:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZonePortalFullAccessPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonDataZonePreviewConsoleFullAccess

Deskripsi: Menyediakan akses penuh ke rilis Pratinjau Amazon DataZone melalui AWS Management Console. Juga menyediakan akses pilih ke layanan terkait lainnya.

`AmazonDataZonePreviewConsoleFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDataZonePreviewConsoleFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 Maret 2023, 15:16 UTC
- Waktu yang telah diedit: 13 Juli 2023, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZonePreviewConsoleFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "datazonecontrol:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "glue:GetConnections",
        "glue:GetDatabase",
        "redshift:DescribeClusters",
        "ec2:DescribeSubnets",
        "secretsmanager:ListSecrets",
        "iam:ListRoles",
        "sso:DescribeRegisteredRegions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateConnection"
```

```
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:connection/AmazonDataZone-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:GetPolicy",
      "Resource" : [
        "arn:aws:iam::*:policy/service-role/AmazonDataZoneBootstrapServicePolicy-
AmazonDataZoneBootstrapRole",
        "arn:aws:iam::*:policy/service-role/AmazonDataZoneServicePolicy-
AmazonDataZoneServiceRole"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/AmazonDataZoneServiceRole*",
        "arn:aws:iam::*:role/service-role/AmazonDataZoneServiceRole*",
        "arn:aws:iam::*:role/AmazonDataZoneBootstrapRole*",
        "arn:aws:iam::*:role/service-role/AmazonDataZoneBootstrapRole",
        "arn:aws:iam::*:role/AmazonDataZoneDomainExecutionRole",
        "arn:aws:iam::*:role/service-role/AmazonDataZoneDomainExecutionRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:passedToService" : "datazonecontrol.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonDataZoneProjectDeploymentPermissionsBoundary

Deskripsi: Amazon DataZone membuat peran IAM yang digunakan untuk menyebarkan proyek analitik data. DataZone menggunakan kebijakan ini saat membuat peran ini untuk menentukan batas izinnya.

`AmazonDataZoneProjectDeploymentPermissionsBoundary`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDataZoneProjectDeploymentPermissionsBoundary` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 21 Maret 2023, 02:54 UTC
- Waktu yang telah diedit: 04 April 2023, 02:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneProjectDeploymentPermissionsBoundary`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:DetachRolePolicy",
        "iam:DeleteRolePolicy",
        "iam:AttachRolePolicy",
        "iam:PutRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/*datazone*",
      "Condition" : {
        "StringEquals" : {
          "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/
AmazonDataZoneProjectRolePermissionsBoundary"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/*datazone*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateKey",
        "kms:TagResource",
        "athena:CreateWorkGroup",
        "athena:TagResource",
        "iam:TagRole",
        "iam:TagPolicy",
        "logs:CreateLogGroup",
        "logs:TagLogGroup",
        "ssm:AddTagsToResource"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : "datazone:*"
        },
        "StringLike" : {
          "aws:ResourceTag/datazone:projectId" : "proj-*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "athena:DeleteWorkGroup",
        "kms:ScheduleKeyDeletion",
        "kms:DescribeKey",
        "kms:EnableKeyRotation",
        "kms:DisableKeyRotation",
        "kms:GenerateDataKey",
        "kms:Encrypt",
        "kms:Decrypt",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/datazone:projectId" : "proj-*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : "datazone:projectId"
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeletePolicy",
        "s3:DeleteBucket"
      ],
      "Resource" : [
        "arn:aws:iam::*:policy/datazone*",
        "arn:aws:s3:::datazone*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter*",
        "ssm:PutParameter",
        "ssm:DeleteParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/*datazone*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetPolicy",
        "iam:GetRolePolicy",
        "iam:CreatePolicy",
        "iam:ListPolicyVersions",
        "lakeformation:RegisterResource",
        "lakeformation:DeregisterResource",
        "lakeformation:GrantPermissions",
        "lakeformation:PutDataLakeSettings",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:RevokePermissions",
        "lakeformation:ListPermissions",
        "glue:CreateDatabase",
        "glue:DeleteDatabase",
        "glue:GetDatabases",
        "glue:GetDatabase",
        "sts:GetCallerIdentity"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/*datazone*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketPublicAccessBlock",
        "s3:DeleteBucketPolicy",
        "s3:CreateBucket",
        "s3:PutBucketPolicy",
        "s3:PutBucketAcl",
        "s3:PutBucketVersioning",
        "s3:PutBucketTagging",
        "s3:PutBucketLogging",
        "s3:GetObject*",
        "s3:GetBucket*",
        "s3:List*",
        "s3:GetEncryptionConfiguration",
        "s3:DeleteObject*",
        "s3:PutObject*",
        "s3:Abort*"
      ],
      "Resource" : "arn:aws:s3:::*datazone*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "athena:Get*",
        "athena:List*",
        "ec2:CreateSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
```

```
        "ec2:DeleteSecurityGroup",
        "ec2:Describe*",
        "ec2:Get*",
        "ec2:List*",
        "logs:PutRetentionPolicy",
        "logs:DescribeLogGroups",
        "logs:DeleteLogGroup",
        "logs:DeleteRetentionPolicy"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:PutKeyPolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "NotResource" : "arn:aws:ec2:*:*:vpc-endpoint/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringLike" : {
          "ec2:VpceServiceName" : [
            "com.amazonaws.*.logs",
            "com.amazonaws.*.s3",
            "com.amazonaws.*.glue",
            "com.amazonaws.*.athena"
          ]
```

```
        }
      }
    },
    {
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:GetTemplate",
        "cloudformation:DescribeChangeSet",
        "cloudformation:CreateChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack",
        "cloudformation:DeleteStack",
        "cloudformation:TagResource",
        "cloudformation:GetTemplateSummary"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*"
      ]
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "s3:GetObject*",
        "s3:GetBucket*",
        "s3:List*",
        "s3:GetEncryptionConfiguration",
        "s3:DeleteObject*",
        "s3:PutObject*",
        "s3:Abort*",
        "s3:DeleteBucket"
      ],
      "NotResource" : [
        "arn:aws:s3:::*datazone*"
      ]
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "kms:*"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Deny",
      "NotAction" : [
        "ssm:PutParameter",
        "ssm:DeleteParameter",
        "ssm:AddTagsToResource",
        "ssm:GetParameters",
        "ssm:GetParameter",
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketPublicAccessBlock",
        "s3:DeleteBucketPolicy",
        "s3:CreateBucket",
        "s3:PutBucketAcl",
        "s3:PutBucketPolicy",
        "s3:PutBucketVersioning",
        "s3:PutBucketTagging",
        "s3:ListBucket",
        "s3:PutBucketLogging",
        "s3:DeleteBucket",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:GetPolicy",
        "iam:CreatePolicy",
        "iam:ListPolicyVersions",
        "iam:DeletePolicy",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:GetTemplate",
        "cloudformation:DescribeChangeSet",
        "cloudformation:CreateChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:TagResource",
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack",
        "cloudformation:DeleteStack",
        "cloudformation:GetTemplateSummary",
```

```
        "athena:*",
        "kms:*",
        "glue:CreateDatabase",
        "glue:DeleteDatabase",
        "glue:GetDatabases",
        "glue:GetDatabase",
        "lambda:*",
        "ec2:*",
        "logs:*",
        "servicecatalog:CreateApplication",
        "servicecatalog:DeleteApplication",
        "servicecatalog:GetApplication",
        "lakeformation:RegisterResource",
        "lakeformation:DeregisterResource",
        "lakeformation:GrantPermissions",
        "lakeformation:PutDataLakeSettings",
        "lakeformation:RevokePermissions",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:ListPermissions",
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:DetachRolePolicy",
        "iam:DeleteRolePolicy",
        "iam:AttachRolePolicy",
        "iam:PutRolePolicy",
        "iam:UntagRole",
        "iam:PassRole",
        "iam:TagRole",
        "s3:GetBucket*",
        "s3:GetObject*",
        "s3:Abort*",
        "s3:GetEncryptionConfiguration",
        "s3:PutObject*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonDataZoneProjectRolePermissionsBoundary

Deskripsi: Amazon DataZone membuat peran IAM untuk proyek untuk melakukan tindakan analitik data, dan menggunakan kebijakan ini saat membuat peran ini untuk menentukan batas izinnya.

`AmazonDataZoneProjectRolePermissionsBoundary`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDataZoneProjectRolePermissionsBoundary` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 21 Maret 2023, 02:51 UTC
- Waktu telah diedit: 21 Maret 2023, 02:51 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneProjectRolePermissionsBoundary`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:List*",
        "s3:Get*",
        "s3:DeleteObjectVersion",
        "s3:RestoreObject",
        "s3:ReplicateObject",
        "s3:PutObject",
        "s3:AbortMultipartUpload",
        "s3:CreateBucket",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutObjectRetention",
        "s3:DeleteObject"
      ],
      "Resource" : "arn:aws:s3:::datazone*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:List*",
        "s3:Get*",
        "kms:List*",
        "kms:Get*",
        "kms:Describe*",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:Describe*",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "logs:*",
        "athena:TerminateSession",
        "athena:CreatePreparedStatement",
        "athena:StopCalculationExecution",
        "athena:StartQueryExecution",
        "athena:UpdatePreparedStatement",
        "athena:BatchGet*",
        "athena:List*",
        "athena:UpdateNotebook",
        "athena:DeleteNotebook",
        "athena:DeletePreparedStatement",
        "athena:UpdateNotebookMetadata",
        "athena:DeleteNamedQuery",
        "athena:Get*",
        "athena:UpdateNamedQuery",
        "athena:CreateNamedQuery",
        "athena:ExportNotebook",
        "athena:StopQueryExecution",
        "athena:StartCalculationExecution",
        "athena:StartSession",
        "athena:CreatePresignedNotebookUrl",
        "athena:CreateNotebook",
        "athena:ImportNotebook",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "lakeformation:GetDataAccess",
        "lakeformation:BatchGrantPermissions",
        "lakeformation:GrantPermissions",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:PutDataLakeSettings",
        "lakeformation:BatchRevokePermissions",
        "lakeformation:GetResourceLFTags",
        "lakeformation:ListPermissions",
        "ram:CreateResourceShare",
        "ram:UpdateResourceShare",
        "ram:DeleteResourceShare",
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare",
        "ram:AcceptResourceShareInvitation",
        "ram:Get*",
        "ram:List*",
```

```
        "redshift:DescribeClusters",
        "redshift:JoinGroup",
        "redshift:CreateClusterUser",
        "redshift:GetClusterCredentials",
        "redshift-data:*",
        "redshift:AuthorizeDataShare",
        "redshift:DescribeDataShares",
        "redshift:AssociateDataShareConsumer",
        "tag:GetResources",
        "iam:ListRoles",
        "iam:ListUsers",
        "iam:ListGroups",
        "iam:ListRolePolicies",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "glue:CreateTable",
        "glue:BatchCreatePartition",
        "glue:CreatePartition",
        "glue:CreatePartitionIndex",
        "glue:CreateDataQualityRuleset",
        "glue:CreateBlueprint",
        "glue:CreateJob",
        "glue:CreateConnection",
        "glue:CreateCrawler",
        "glue:CreateWorkflow",
        "sqlworkbench:*",
        "datazone:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws-glue-service-resource"
          ]
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:List*",
        "kms:Get*",
        "kms:Describe*",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:ReEncrypt*",
        "kms:Verify",
        "kms:Sign",
        "kms:GenerateDataKey",
        "glue:*"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/datazone:projectId" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:BatchGet*",
        "glue:SearchTables",
        "glue:List*",
        "glue:Get*",
        "glue:CreateDatabase",
        "glue:UpdateDatabase",
        "glue:DeleteTable",
        "glue:BatchDeleteTable",
```

```
        "glue:UpdateTable",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
        "glue:PutResourcePolicy",
        "glue:BatchUpdatePartition",
        "glue:DeleteTableVersion",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeletePartitionIndex",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:BatchDeleteTableVersion",
        "glue:UpdatePartition",
        "glue:NotifyEvent",
        "glue:DeleteResourcePolicy"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Deny",
      "NotAction" : [
        "s3:List*",
        "s3:Get*",
        "s3:Describe*",
        "s3:DeleteObjectVersion",
        "s3:RestoreObject",
        "s3:ReplicateObject",
        "s3:PutObject",
        "s3:AbortMultipartUpload",
        "s3:CreateBucket",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutObjectRetention",
        "s3:DeleteObject",
        "kms:List*",
        "kms:Get*",
        "kms:Describe*",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:ReEncrypt*",
        "kms:Verify",
        "kms:Sign",
        "kms:GenerateDataKey",
        "ec2:Describe*",
        "ec2:CreateNetworkInterface",
```

```
        "ec2:DeleteNetworkInterface",
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "logs:*",
        "athena:*",
        "glue:BatchGet*",
        "glue:Get*",
        "glue:SearchTables",
        "glue:List*",
        "glue:CreateDatabase",
        "glue:UpdateDatabase",
        "glue:CreateTable",
        "glue:DeleteTable",
        "glue:BatchDeleteTable",
        "glue:UpdateTable",
        "glue:BatchCreatePartition",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
        "glue:PutResourcePolicy",
        "glue:CreatePartitionIndex",
        "glue:BatchUpdatePartition",
        "glue:DeleteTableVersion",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeletePartitionIndex",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:BatchDeleteTableVersion",
        "glue:UpdatePartition",
        "glue:NotifyEvent",
        "glue:StartBlueprintRun",
        "glue:PutWorkflowRunProperties",
        "glue:StopCrawler",
        "glue:DeleteJob",
        "glue:DeleteWorkflow",
        "glue:UpdateCrawler",
        "glue:DeleteBlueprint",
        "glue:UpdateWorkflow",
        "glue:StartCrawler",
        "glue:ResetJobBookmark",
        "glue:UpdateJob",
        "glue:StartWorkflowRun",
        "glue:StopCrawlerSchedule",
```

```
        "glue:ResumeWorkflowRun",
        "glue:DeleteCrawler",
        "glue:UpdateBlueprint",
        "glue:BatchStopJobRun",
        "glue:StopWorkflowRun",
        "glue:UpdateCrawlerSchedule",
        "glue:DeleteConnection",
        "glue:UpdateConnection",
        "glue:BatchDeleteConnection",
        "glue:StartCrawlerSchedule",
        "glue:StartJobRun",
        "glue:CreateWorkflow",
        "glue:*DataQuality*",
        "glue:CreateBlueprint",
        "glue:CreateJob",
        "glue:CreateConnection",
        "glue:CreateCrawler",
        "glue:DeleteResourcePolicy",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "lakeformation:GetDataAccess",
        "lakeformation:BatchGrantPermissions",
        "lakeformation:GrantPermissions",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:PutDataLakeSettings",
        "lakeformation:BatchRevokePermissions",
        "lakeformation:GetResourceLFTags",
        "lakeformation:ListPermissions",
        "ram:*",
        "redshift:*",
        "redshift-data:*",
        "tag:GetResources",
        "iam:List*",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:PassRole",
        "sqlworkbench:*",
        "datazone:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonDataZoneRedshiftGlueProvisioningPolicy

Deskripsi: Amazon DataZone adalah layanan manajemen data yang memungkinkan Anda membuat katalog, menemukan, mengatur, berbagi, dan menganalisis data Anda. Dengan Amazon DataZone, Anda dapat berbagi dan mengakses data Anda di seluruh akun dan wilayah yang didukung. Amazon DataZone menyederhanakan pengalaman Anda di seluruh AWS layanan, termasuk, namun tidak terbatas pada, Amazon Redshift, Amazon Athena, AWS Glue, dan Lake Formation. AWS

`AmazonDataZoneRedshiftGlueProvisioningPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDataZoneRedshiftGlueProvisioningPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 22 September 2023, 20:19 UTC
- Waktu yang telah diedit: 23 Oktober 2024, 18:29 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneRedshiftGlueProvisioningPolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

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

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

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

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

```
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentIAMPolicyManagement",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeletePolicy",
        "iam:CreatePolicy",
        "iam:GetPolicy",
        "iam:ListPolicyVersions",
        "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*"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonDataZoneRedshiftManageAccessRolePolicy

Deskripsi: Kebijakan ini memberikan DataZone izin Amazon untuk mempublikasikan data Amazon Redshift ke katalog. Ini juga memberikan DataZone izin Amazon untuk memberikan akses atau mencabut akses ke Amazon Redshift atau Amazon Redshift Serverless aset yang diterbitkan dalam katalog.

`AmazonDataZoneRedshiftManageAccessRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDataZoneRedshiftManageAccessRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 22 September 2023, 20:15 UTC
- Waktu telah diedit: 07 Maret 2025, 00:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneRedshiftManageAccessRolePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary

Deskripsi: AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary Kebijakan ini adalah daftar izin yang diizinkan pada peran eksekusi yang dibuat di SageMaker lingkungan yang disediakan oleh Amazon. DataZone

`AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 23 April 2024, 23:01 UTC
- Waktu telah diedit: November 21, 2024, 23:06 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowAllNonAdminSageMakerActions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:*",
        "sagemaker-geospatial:*"
      ],
      "NotResource" : [
        "arn:aws:sagemaker:*:*:domain/*",
        "arn:aws:sagemaker:*:*:user-profile/*",
        "arn:aws:sagemaker:*:*:app/*",
        "arn:aws:sagemaker:*:*:space/*",
        "arn:aws:sagemaker:*:*:flow-definition/*"
      ]
    },
    {
      "Sid" : "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",
        "elastic-inference:Connect",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListClusters",
        "events:PutRule",
        "events:DescribeRule",
        "events:PutTargets",
        "events:TagResource",
        "events:ListTagsForResource",
        "fsx:DescribeFileSystems",
        "glue:SearchTables",
        "glue:NotifyEvent",
        "glue:StartBlueprintRun",
        "glue:PutWorkflowRunProperties",
        "glue:StopCrawler",
        "glue:DeleteJob",
        "glue:DeleteWorkflow",
        "glue:UpdateCrawler",
```

```
        "glue:DeleteBlueprint",
        "glue:UpdateWorkflow",
        "glue:StartCrawler",
        "glue:ResetJobBookmark",
        "glue:UpdateJob",
        "glue:StartWorkflowRun",
        "glue:StopCrawlerSchedule",
        "glue:ResumeWorkflowRun",
        "glue:DeleteCrawler",
        "glue:UpdateBlueprint",
        "glue:BatchStopJobRun",
        "glue:StopWorkflowRun",
        "glue:BatchGet*",
        "glue:UpdateCrawlerSchedule",
        "glue:DeleteConnection",
        "glue:UpdateConnection",
        "glue:Get*",
        "glue:BatchDeleteConnection",
        "glue:StartCrawlerSchedule",
        "glue:StartJobRun",
        "glue:CreateWorkflow",
        "glue:*DataQuality*",
        "glue:List*",
        "glue:CreateSession",
        "glue:RunStatement",
        "glue:BatchCreatePartition",
        "glue:CreateDatabase",
        "glue:CreatePartitionIndex",
        "glue:CreateTable",
        "glue:BatchUpdatePartition",
        "glue:BatchDeletePartition",
        "glue:UpdateTable",
        "glue:DeleteTableVersion",
        "glue:DeleteTable",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeletePartitionIndex",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:BatchDeleteTableVersion",
        "glue:BatchDeleteTable",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:UpdatePartition",
```

```
        "glue:CreateBlueprint",
        "glue:CreateJob",
        "glue:CreateConnection",
        "glue:CreateCrawler",
        "groundtruthlabeling:*",
        "iam:CreateServiceLinkedRole",
        "iam:GetRole",
        "iam:ListRoles",
        "iam:PassRole",
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:Decrypt",
        "kms:ListKeys",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:RetireGrant",
        "lakeformation:GetDataAccess",
        "lambda:ListFunctions",
        "lambda:InvokeFunction",
        "logs:CreateLogDelivery",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DeleteLogDelivery",
        "logs:Describe*",
        "logs:GetLogDelivery",
        "logs:GetLogEvents",
        "logs:ListLogDeliveries",
        "logs:PutLogEvents",
        "logs:UpdateLogDelivery",
        "ram:AcceptResourceShareInvitation",
        "rds:DescribeDBInstances",
        "redshift:CreateClusterUser",
        "redshift:GetClusterCredentials",
        "redshift:GetClusterCredentialsWithIAM",
        "redshift:DescribeClusters",
        "redshift-data:BatchExecuteStatement",
        "redshift-data:CancelStatement",
        "redshift-data:DescribeStatement",
        "redshift-data:DescribeTable",
        "redshift-data:ExecuteStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables",
        "redshift-serverless:ListNamespaces",
```

```
        "redshift-serverless:ListWorkgroups",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:GetCredentials",
        "s3:GetBucketAcl",
        "s3:PutObjectAcl",
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:AbortMultipartUpload",
        "s3:CreateBucket",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketCors",
        "s3:PutBucketCors",
        "s3:DeleteObjectVersion",
        "s3:PutObjectRetention",
        "s3:ReplicateObject",
        "s3:RestoreObject",
        "secretsmanager:ListSecrets",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:CreateSecret",
        "secretsmanager:PutResourcePolicy",
        "secretsmanager:TagResource",
        "servicecatalog:Describe*",
        "servicecatalog:List*",
        "servicecatalog:ScanProvisionedProducts",
        "servicecatalog:SearchProducts",
        "servicecatalog:SearchProvisionedProducts",
        "servicecatalog:ProvisionProduct",
        "servicecatalog:TerminateProvisionedProduct",
        "servicecatalog:UpdateProvisionedProduct",
        "sns:ListTopics",
        "sns:Subscribe",
        "sns:CreateTopic",
        "sns:Publish",
        "states:DescribeExecution",
        "states:GetExecutionHistory",
        "states:StartExecution",
        "states:StopExecution",
        "states:UpdateStateMachine",
        "tag:GetResources",
```

```
        "sso:CreateApplicationAssignment",
        "sso:AssociateProfile"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonDataZoneSageMakerManageAccessRolePolicy

Deskripsi: AmazonDataZoneSageMakerManageAccessRolePolicy Kebijakan ini memberi Amazon izin DataZone yang diperlukan untuk memberikan akses pengguna ke berbagai sumber daya di SageMaker lingkungan.

`AmazonDataZoneSageMakerManageAccessRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDataZoneSageMakerManageAccessRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 23 April 2024, 23:34 UTC
- Waktu telah diedit: November 21, 2024, 20:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneSageMakerManageAccessRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonDataZoneSageMakerProvisioningRolePolicy

Deskripsi: AmazonDataZoneSageMakerProvisioningRolePolicy Kebijakan ini memberi Amazon izin DataZone yang diperlukan untuk berinteraksi dengan Amazon. SageMaker

`AmazonDataZoneSageMakerProvisioningRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDataZoneSageMakerProvisioningRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 23 April 2024, 23:32 UTC
- Waktu telah diedit: 09 Januari 2025, 20:52 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneSageMakerProvisioningRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonDetectiveFullAccess

Deskripsi: Menyediakan akses penuh ke layanan Detektif Amazon dan akses cakupan ke dependensi UI konsol

`AmazonDetectiveFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDetectiveFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 April 2020, 17:57 UTC
- Waktu telah diedit: 17 Mei 2023, 19:39 UTC

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

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "detective:*",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "guardduty:ArchiveFindings"
      ],
      "Resource" : "arn:aws:guardduty:*:*:detector/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "guardduty:GetFindings",
        "guardduty:ListDetectors"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "securityHub:GetFindings"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonDetectiveInvestigatorAccess

Deskripsi: Menyediakan akses penyidik ke layanan Detektif Amazon dan akses cakupan ke dependensi UI konsol. Kebijakan ini memberikan izin untuk menyelam ke Detektif untuk tujuan investigasi dan akses tulis terbatas ke Guardduty.

`AmazonDetectiveInvestigatorAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDetectiveInvestigatorAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 17 Januari 2023, 15:24 UTC
- Waktu telah diedit: 27 November 2023, 03:13 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDetectiveInvestigatorAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DetectivePermissions",
      "Effect" : "Allow",
      "Action" : [
        "detective:BatchGetGraphMemberDatasources",
        "detective:BatchGetMembershipDatasources",
        "detective:DescribeOrganizationConfiguration",
        "detective:GetFreeTrialEligibility",
        "detective:GetGraphIngestState",
        "detective:GetMembers",
        "detective:GetPricingInformation",
        "detective:GetUsageInformation",
        "detective:ListDatasourcePackages",
        "detective:ListGraphs",
        "detective:ListHighDegreeEntities",
        "detective:ListInvitations",
        "detective:ListMembers",
        "detective:ListOrganizationAdminAccount",
        "detective:ListTagsForResource",
        "detective:SearchGraph",
        "detective:StartInvestigation",
        "detective:GetInvestigation",
        "detective:ListInvestigations",
        "detective:UpdateInvestigationState",
        "detective:ListIndicators",
        "detective:InvokeAssistant"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
```

```
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GuardDutyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "guardduty:ArchiveFindings",
        "guardduty:GetFindings",
        "guardduty:ListDetectors"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityHubPermissions",
      "Effect" : "Allow",
      "Action" : [
        "securityHub:GetFindings"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonDetectiveMemberAccess

Deskripsi: Menyediakan akses anggota ke layanan Detektif Amazon dan akses cakupan ke dependensi UI konsol.

`AmazonDetectiveMemberAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDetectiveMemberAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 17 Januari 2023, 15:16 UTC
- Waktu yang telah diedit: 17 Januari 2023, 15:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDetectiveMemberAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "detective:AcceptInvitation",
        "detective:BatchGetMembershipDatasources",
        "detective:DisassociateMembership",
        "detective:GetFreeTrialEligibility",
        "detective:GetPricingInformation",
        "detective:GetUsageInformation",
        "detective:ListInvitations",
        "detective:RejectInvitation"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonDetectiveOrganizationsAccess

Deskripsi: Menyediakan akses Organizations untuk mengelola administrator Delegasi untuk Amazon Detective dan akses cakupan ke dependensi UI konsol. Ini juga memberikan izin untuk membuat peran terkait layanan untuk Detektif.

`AmazonDetectiveOrganizationsAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDetectiveOrganizationsAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 02 Maret 2023, 15:20 UTC
- Waktu telah diedit: 02 Maret 2023, 15:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDetectiveOrganizationsAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "detective:DisableOrganizationAdminAccount",
        "detective:EnableOrganizationAdminAccount",
        "detective:ListOrganizationAdminAccount"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "detective.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "detective.amazonaws.com"
          ]
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "detective.amazonaws.com",
            "guardduty.amazonaws.com",
            "macie.amazonaws.com",
            "securityhub.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonDetectiveServiceLinkedRolePolicy

Deskripsi: Memungkinkan Amazon Detective untuk melakukan panggilan layanan atas nama Anda

`AmazonDetectiveServiceLinkedRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 18 November 2021 19:47 UTC
- Waktu yang telah diedit: 18 November 2021 19:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonDetectiveServiceLinkedRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonDevOpsGuruConsoleFullAccess

Deskripsi: Kebijakan memberikan akses penuh ke konsol DevOps Guru.

`AmazonDevOpsGuruConsoleFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDevOpsGuruConsoleFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 17 Desember 2021 18:43 UTC
- Waktu yang telah diedit: 25 Agustus 2022, 18.18 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDevOpsGuruConsoleFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      "Effect" : "Allow",
      "Action" : [
        "devops-guru:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudFormationListStacksAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchGetMetricDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SnsListTopicsAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SnsTopicOperations",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:GetTopicAttributes",
        "sns:SetTopicAttributes",
        "sns:Publish"
      ],
      "Resource" : "arn:aws:sns:*:*:DevOps-Guru-*"
    },
    {
      "Sid" : "DevOpsGuruSlrCreation",
```

```
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/devops-guru.amazonaws.com/
AWSServiceRoleForDevOpsGuru",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "devops-guru.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DevOpsGuruSlrDeletion",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/devops-guru.amazonaws.com/
AWSServiceRoleForDevOpsGuru"
    },
    {
      "Sid" : "RDSDescribeDBInstancesAccess",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PerformanceInsightsMetricsDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "pi:GetResourceMetrics",
        "pi:DescribeDimensionKeys"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchLogsFilterLogEventsAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:FilterLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/DevOps-Guru-Analysis" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonDevOpsGuruFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon DevOps Guru.

`AmazonDevOpsGuruFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDevOpsGuruFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Desember 2020, 16:38 UTC
- Waktu yang telah diedit: 25 Agustus 2022, 18.23 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDevOpsGuruFullAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DevOpsGuruFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "devops-guru:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudFormationListStacksAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchGetMetricDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SnsListTopicsAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "SnsTopicOperations",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:GetTopicAttributes",
        "sns:SetTopicAttributes",
        "sns:Publish"
      ],
      "Resource" : "arn:aws:sns:*:*:DevOps-Guru-*"
    },
    {
      "Sid" : "DevOpsGuruSlrCreation",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/devops-guru.amazonaws.com/
AWSServiceRoleForDevOpsGuru",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "devops-guru.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DevOpsGuruSlrDeletion",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/devops-guru.amazonaws.com/
AWSServiceRoleForDevOpsGuru"
    },
    {
      "Sid" : "RDSDescribeDBInstancesAccess",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchLogsFilterLogEventsAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "logs:FilterLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/DevOps-Guru-Analysis" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonDevOpsGuruOrganizationsAccess

Deskripsi: Menyediakan akses untuk mengaktifkan dan mengelola Amazon DevOps Guru dalam suatu organisasi.

`AmazonDevOpsGuruOrganizationsAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDevOpsGuruOrganizationsAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 15 November 2021 23:50 UTC
- Waktu yang telah diedit: 15 November 2021, 23:50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDevOpsGuruOrganizationsAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DevOpsGuruOrganizationsAccess",
      "Effect" : "Allow",
      "Action" : [
        "devops-guru:DescribeOrganizationHealth",
        "devops-guru:DescribeOrganizationResourceCollectionHealth",
        "devops-guru:DescribeOrganizationOverview",
        "devops-guru:ListOrganizationInsights",
        "devops-guru:SearchOrganizationInsights"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationsDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListAccounts",
        "organizations:ListChildren",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListRoots"
      ],
      "Resource" : "arn:aws:organizations::*:"
    },
    {
      "Sid" : "OrganizationsAdminDataAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "organizations:DeregisterDelegatedAdministrator",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators",
        "organizations:EnableAWSServiceAccess",
        "organizations:DisableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "devops-guru.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonDevOpsGuruReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon DevOps Guru Console.

`AmazonDevOpsGuruReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDevOpsGuruReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Desember 2020, 16:34 UTC

- Waktu yang telah diedit: 25 Agustus 2022, 18.11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDevOpsGuruReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DevOpsGuruReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "devops-guru:DescribeAccountHealth",
        "devops-guru:DescribeAccountOverview",
        "devops-guru:DescribeAnomaly",
        "devops-guru:DescribeEventSourcesConfig",
        "devops-guru:DescribeFeedback",
        "devops-guru:DescribeInsight",
        "devops-guru:DescribeResourceCollectionHealth",
        "devops-guru:DescribeServiceIntegration",
        "devops-guru:GetCostEstimation",
        "devops-guru:GetResourceCollection",
        "devops-guru:ListAnomaliesForInsight",
        "devops-guru:ListEvents",
        "devops-guru:ListInsights",
        "devops-guru:ListAnomalousLogGroups",
        "devops-guru:ListMonitoredResources",
        "devops-guru:ListNotificationChannels",
        "devops-guru:ListRecommendations",
        "devops-guru:SearchInsights",
        "devops-guru:StartCostEstimation"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "CloudFormationListStacksAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/devops-guru.amazonaws.com/
AWSServiceRoleForDevOpsGuru"
    },
    {
      "Sid" : "CloudWatchGetMetricDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RDSDescribeDBInstancesAccess",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchLogsFilterLogEventsAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:FilterLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/DevOps-Guru-Analysis" : "true"
        }
```

```
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonDevOpsGuruServiceRolePolicy

Deskripsi: Peran terkait layanan yang diperlukan Amazon DevOpsGuru untuk mengakses sumber daya Anda.

`AmazonDevOpsGuruServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 01 Desember 2020, 10:24 UTC
- Waktu telah diedit: 10 Januari 2023, 14:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonDevOpsGuruServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAutoScalingGroups",
        "cloudtrail:LookupEvents",
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics",
        "cloudwatch:DescribeAnomalyDetectors",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:ListDashboards",
        "cloudwatch:GetDashboard",
        "cloudformation:GetTemplate",
        "cloudformation:ListStacks",
        "cloudformation:ListStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:ListImports",
        "codedeploy:BatchGetDeployments",
        "codedeploy:GetDeploymentGroup",
        "codedeploy:ListDeployments",
        "config:DescribeConfigurationRecorderStatus",
        "config:GetResourceConfigHistory",
        "events:ListRuleNamesByTarget",
        "xray:GetServiceGraph",
        "organizations:ListRoots",
        "organizations:ListChildren",
        "organizations:ListDelegatedAdministrators",
        "pi:GetResourceMetrics",
        "tag:GetResources",
        "lambda:GetFunction",
        "lambda:GetFunctionConcurrency",
        "lambda:GetAccountSettings",
        "lambda:ListProvisionedConcurrencyConfigs",
        "lambda:ListAliases",
        "lambda:ListEventSourceMappings",
```

```
        "lambda:GetPolicy",
        "ec2:DescribeSubnets",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "sqs:GetQueueAttributes",
        "kinesis:DescribeStream",
        "kinesis:DescribeLimits",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeStream",
        "dynamodb:ListStreams",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "rds:DescribeOptionGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBInstanceAutomatedBackups",
        "rds:DescribeAccountAttributes",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "s3:GetBucketNotification",
        "s3:GetBucketPolicy",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketTagging",
        "s3:GetBucketWebsite",
        "s3:GetIntelligentTieringConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetReplicationConfiguration",
        "s3:ListAllMyBuckets",
        "s3:ListStorageLensConfigurations",
        "servicequotas:GetServiceQuota",
        "servicequotas:ListRequestedServiceQuotaChangeHistory",
        "servicequotas:ListServiceQuotas"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowPutTargetsOnASpecificRule",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:PutRule"
```

```
      ],
      "Resource" : "arn:aws:events:*:*:rule/DevOps-Guru-managed-*"
    },
    {
      "Sid" : "AllowCreateOpsItem",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateOpsItem"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAddTagsToOpsItem",
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:opsitem/*"
    },
    {
      "Sid" : "AllowAccessOpsItem",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetOpsItem",
        "ssm:UpdateOpsItem"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/DevOps-GuruInsightSsmOpsItemRelated" : "true"
        }
      }
    },
    {
      "Sid" : "AllowCreateManagedRule",
      "Effect" : "Allow",
      "Action" : "events:PutRule",
      "Resource" : "arn:aws:events:*:*:rule/DevOpsGuruManagedRule*"
    },
    {
      "Sid" : "AllowAccessManagedRule",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
```

```
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/DevOpsGuruManagedRule*"
    },
    {
      "Sid" : "AllowOtherOperationsOnManagedRule",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:EnableRule",
        "events:DisableRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/DevOpsGuruManagedRule*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "devops-guru.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowTagBasedFilterLogEvents",
      "Effect" : "Allow",
      "Action" : [
        "logs:FilterLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/DevOps-Guru-Analysis" : "true"
        }
      }
    },
    {
      "Sid" : "AllowAPIGatewayGetIntegrations",
      "Effect" : "Allow",
      "Action" : "apigateway:GET",
      "Resource" : [
        "arn:aws:apigateway:*::/restapis/??????????",
        "arn:aws:apigateway:*::/restapis/*/resources",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integration"
      ]
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonDMSCloudWatchLogsRole

Deskripsi: Menyediakan akses untuk mengunggah log replikasi DMS ke log cloudwatch di akun pelanggan.

`AmazonDMSCloudWatchLogsRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDMSCloudWatchLogsRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 07 Januari 2016, 23:44 UTC
- Waktu yang telah diedit: 23 Mei 2023, 21:32 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDMSCloudWatchLogsRole`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
  "Statement" : [
    {
      "Sid" : "AllowDescribeOnAllLogGroups",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowDescribeOfAllLogStreamsOnDmsTasksLogGroup",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:dms-tasks-*",
        "arn:aws:logs:*:*:log-group:dms-serverless-replication-*"
      ]
    },
    {
      "Sid" : "AllowCreationOfDmsLogGroups",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:dms-tasks-*",
        "arn:aws:logs:*:*:log-group:dms-serverless-replication-*:log-stream:"
      ]
    },
    {
      "Sid" : "AllowCreationOfDmsLogStream",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:dms-tasks-*:log-stream:dms-task-*",
        "arn:aws:logs:*:*:log-group:dms-serverless-replication-*:log-stream:dms-
serverless-*"
      ]
```

```
    },
    {
      "Sid" : "AllowUploadOfLogEventsToDmsLogStream",
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:dms-tasks-*:log-stream:dms-task-*",
        "arn:aws:logs:*:*:log-group:dms-serverless-replication-*:log-stream:dms-
serverless-*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonDMSRedshiftS3Role

Deskripsi: Menyediakan akses untuk mengelola pengaturan S3 untuk titik akhir Redshift untuk DMS.

`AmazonDMSRedshiftS3Role`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDMSRedshiftS3Role` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 20 April 2016, 17:05 UTC
- Waktu yang telah diedit: 08 Juli 2019, 18:19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDMSRedshiftS3Role`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:ListBucket",
        "s3:DeleteBucket",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:GetObjectVersion",
        "s3:GetBucketPolicy",
        "s3:PutBucketPolicy",
        "s3:GetBucketAcl",
        "s3:PutBucketVersioning",
        "s3:GetBucketVersioning",
        "s3:PutLifecycleConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:DeleteBucketPolicy"
      ],
      "Resource" : "arn:aws:s3:::dms-*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonDMSVPCManagementRole

Deskripsi: Menyediakan akses untuk mengelola pengaturan VPC untuk konfigurasi pelanggan AWS terkelola

`AmazonDMSVPCManagementRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDMSVPCManagementRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 18 November 2015, 16:33 UTC
- Waktu yang telah diedit: 25 Juli 2024, 15:19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDMSVPCManagementRole`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonDocDB-ElasticServiceRolePolicy

Deskripsi: Memungkinkan Amazon DocumentDB-Elastic mengelola AWS sumber daya atas nama Anda.

`AmazonDocDB-ElasticServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan

- Waktu pembuatan: 30 November 2022, 14:17 UTC
- Waktu yang telah diedit: 30 November 2022, 14.17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonDocDB-ElasticServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonDocDBConsoleFullAccess

Deskripsi: Menyediakan akses penuh untuk mengelola Amazon DocumentDB dengan kompatibilitas MongoDB menggunakan file. AWS Management Console Perhatikan kebijakan ini juga memberikan akses penuh untuk mempublikasikan semua topik SNS dalam akun, izin untuk membuat dan mengedit EC2 instans Amazon dan konfigurasi VPC, izin untuk melihat dan mencantumkan kunci di Amazon KMS, dan akses penuh ke Amazon RDS dan Amazon Neptunus.

`AmazonDocDBConsoleFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDocDBConsoleFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 09 Januari 2019, 20:37 UTC
- Waktu yang telah diedit: 11 Februari 2025, 18:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBConsoleFullAccess`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "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"
        }
```

```
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonDocDBElasticFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon DocumentDB Elastic Clusters dan izin lain yang diperlukan untuk EC2 dependensinya termasuk, KMS, dan IAM. SecretsManager CloudWatch

`AmazonDocDBElasticFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDocDBElasticFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 05 Juni 2023, 13:51 UTC
- Waktu yang telah diedit: 11 Februari 2025, 18:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBElasticFullAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonDocDBElasticReadOnlyAccess

Deskripsi: Menyediakan akses hanya-baca ke Amazon DocDB-elastis dan metrik. CloudWatch

`AmazonDocDBElasticReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDocDBElasticReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 08 Juni 2023, 14:37 UTC
- Waktu yang telah diedit: 21 Juni 2023, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBElasticReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "docdb-elastic:ListClusters",
        "docdb-elastic:GetCluster",
        "docdb-elastic:ListClusterSnapshots",
        "docdb-elastic:GetClusterSnapshot",
        "docdb-elastic:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonDocDBFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon DocumentDB dengan kompatibilitas MongoDB. Perhatikan kebijakan ini juga memberikan akses penuh untuk mempublikasikan semua topik SNS dalam akun dan akses penuh ke Amazon RDS dan Amazon Neptunus.

`AmazonDocDBFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDocDBFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 09 Januari 2019, 20:21 UTC
- Waktu yang telah diedit: 09 Januari 2019, 20:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "rds:AddRoleToDBCluster",
        "rds:AddSourceIdentifierToSubscription",
        "rds:AddTagsToResource",
        "rds:ApplyPendingMaintenanceAction",
        "rds:CopyDBClusterParameterGroup",
        "rds:CopyDBClusterSnapshot",
```

```
        "rds:CopyDBParameterGroup",
        "rds:CreateDBCluster",
        "rds:CreateDBClusterParameterGroup",
        "rds:CreateDBClusterSnapshot",
        "rds:CreateDBInstance",
        "rds:CreateDBParameterGroup",
        "rds:CreateDBSubnetGroup",
        "rds:CreateEventSubscription",
        "rds:DeleteDBCluster",
        "rds:DeleteDBClusterParameterGroup",
        "rds:DeleteDBClusterSnapshot",
        "rds:DeleteDBInstance",
        "rds:DeleteDBParameterGroup",
        "rds:DeleteDBSubnetGroup",
        "rds:DeleteEventSubscription",
        "rds:DescribeAccountAttributes",
        "rds:DescribeCertificates",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBLogFiles",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultClusterParameters",
        "rds:DescribeEngineDefaultParameters",
        "rds:DescribeEventCategories",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeEvents",
        "rds:DescribeOptionGroups",
        "rds:DescribeOrderableDBInstanceOptions",
        "rds:DescribePendingMaintenanceActions",
        "rds:DescribeValidDBInstanceModifications",
        "rds:DownloadDBLogFilePortion",
        "rds:FailoverDBCluster",
        "rds:ListTagsForResource",
        "rds:ModifyDBCluster",
        "rds:ModifyDBClusterParameterGroup",
        "rds:ModifyDBClusterSnapshotAttribute",
```

```
        "rds:ModifyDBInstance",
        "rds:ModifyDBParameterGroup",
        "rds:ModifyDBSubnetGroup",
        "rds:ModifyEventSubscription",
        "rds:PromoteReadReplicaDBCluster",
        "rds:RebootDBInstance",
        "rds:RemoveRoleFromDBCluster",
        "rds:RemoveSourceIdentifierFromSubscription",
        "rds: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"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonDocDBReadOnlyAccess

Deskripsi: Menyediakan akses hanya-baca ke Amazon DocumentDB dengan kompatibilitas MongoDB. Perhatikan bahwa kebijakan ini juga memberikan akses ke sumber daya Amazon RDS dan Amazon Neptunus.

`AmazonDocDBReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDocDBReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 09 Januari 2019, 20:30 UTC
- Waktu yang telah diedit: 09 Januari 2019, 20:30 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "rds:DescribeAccountAttributes",
        "rds:DescribeCertificates",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBLogFiles",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEventCategories",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeEvents",
        "rds:DescribeOrderableDBInstanceOptions",
        "rds:DescribePendingMaintenanceActions",
        "rds:DownloadDBLogFilePortion",
        "rds:ListTagsForResource"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
```

```
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "kms:ListKeys",
        "kms:ListRetirableGrants",
        "kms:ListAliases",
        "kms:ListKeyPolicies"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:GetLogEvents"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/rds/*:log-stream:*",
        "arn:aws:logs:*:*:log-group:/aws/docdb/*:log-stream:*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonDRSVPCManagement

Deskripsi: Menyediakan akses untuk mengelola pengaturan VPC untuk konfigurasi pelanggan terkelola Amazon

`AmazonDRSVPCManagement`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDRSVPCManagement` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 02 September 2015, 00:09 UTC
- Waktu telah diedit: 02 September 2015, 00:09 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDRSVPCManagement`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonDynamoDBFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon DynamoDB melalui file. AWS Management Console

`AmazonDynamoDBFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDynamoDBFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu yang telah diedit: 29 Januari 2021 17:38 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDynamoDBFullAccess`

Versi kebijakan

Versi kebijakan: v15 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "dynamodb:*",
        "dax:*",
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:GetMetricData",
        "datapipeline:ActivatePipeline",
```

```
        "datapipeline:CreatePipeline",
        "datapipeline:DeletePipeline",
        "datapipeline:DescribeObjects",
        "datapipeline:DescribePipelines",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:ListPipelines",
        "datapipeline:PutPipelineDefinition",
        "datapipeline:QueryObjects",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "iam:GetRole",
        "iam:ListRoles",
        "kms:DescribeKey",
        "kms:ListAliases",
        "sns:CreateTopic",
        "sns:DeleteTopic",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "sns:Subscribe",
        "sns:Unsubscribe",
        "sns:SetTopicAttributes",
        "lambda:CreateFunction",
        "lambda:ListFunctions",
        "lambda:ListEventSourceMappings",
        "lambda:CreateEventSourceMapping",
        "lambda:DeleteEventSourceMapping",
        "lambda:GetFunctionConfiguration",
        "lambda:DeleteFunction",
        "resource-groups:ListGroups",
        "resource-groups:ListGroupResources",
        "resource-groups:GetGroup",
        "resource-groups:GetGroupQuery",
        "resource-groups:DeleteGroup",
        "resource-groups:CreateGroup",
        "tag:GetResources",
        "kinesis:ListStreams",
        "kinesis:DescribeStream",
        "kinesis:DescribeStreamSummary"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
```

```
    {
      "Action" : "cloudwatch:GetInsightRuleReport",
      "Effect" : "Allow",
      "Resource" : "arn:aws:cloudwatch:*:*:insight-rule/DynamoDBContributorInsights*"
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "application-autoscaling.amazonaws.com",
            "application-autoscaling.amazonaws.com.cn",
            "dax.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "replication.dynamodb.amazonaws.com",
            "dax.amazonaws.com",
            "dynamodb.application-autoscaling.amazonaws.com",
            "contributorinsights.dynamodb.amazonaws.com",
            "kinesisreplication.dynamodb.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonDynamoDBFullAccess_v2

Deskripsi: Menyediakan akses penuh ke Amazon DynamoDB

`AmazonDynamoDBFullAccess_v2`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDynamoDBFullAccess_v2` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 22 Mei 2025, 14:52 UTC
- Waktu yang telah diedit: 22 Mei 2025, 14:52 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDynamoDBFullAccess_v2`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonDynamoDBFullAccesswithDataPipeline

Deskripsi: Kebijakan ini berada di jalur penghentian. Lihat dokumentasi untuk panduan: https:// docs.aws.amazon.com/amazondynamodb/ latest/developerguide/DynamoDBPipeline.html. Provides full access to Amazon DynamoDB including Export/Import menggunakan AWS Data Pipeline melalui AWS Management Console.

`AmazonDynamoDBFullAccesswithDataPipeline`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDynamoDBFullAccesswithDataPipeline` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu telah diedit: 12 November 2015, 02:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDynamoDBFullAccesswithDataPipeline`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:PutMetricAlarm",
        "dynamodb:*",
        "sns:CreateTopic",
        "sns:DeleteTopic",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "sns:Subscribe",
        "sns:Unsubscribe",
        "sns:SetTopicAttributes"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Sid" : "DDBConsole"
    },
    {
      "Action" : [
        "lambda:*",
        "iam:ListRoles"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Sid" : "DDBConsoleTriggers"
    },
    {
      "Action" : [
```

```
        "datapipeline:*",
        "iam:ListRoles"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Sid" : "DDBConsoleImportExport"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRolePolicy",
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Sid" : "IAMEDPRoles"
    },
    {
      "Action" : [
        "ec2:CreateTags",
        "ec2:DescribeInstances",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "elasticmapreduce:*",
        "datapipeline:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Sid" : "EMR"
    },
    {
      "Action" : [
        "s3:DeleteObject",
        "s3:Get*",
        "s3:List*",
        "s3:Put*"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ],
```

```
      "Sid" : "S3"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonDynamoDBReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon DynamoDB melalui file. AWS Management Console

`AmazonDynamoDBReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDynamoDBReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu telah diedit: November 18, 2024, 17:38 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDynamoDBReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v15 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GeneralReadOnlyAccess",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricData",
        "datapipeline:DescribeObjects",
        "datapipeline:DescribePipelines",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:ListPipelines",
        "datapipeline:QueryObjects",
        "dynamodb:BatchGetItem",
        "dynamodb:Describe*",
        "dynamodb:List*",
        "dynamodb: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*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonEBSCSIDriverPolicy

Deskripsi: Kebijakan IAM yang memungkinkan akun layanan driver CSI untuk melakukan panggilan ke layanan terkait seperti EC2 atas nama Anda.

`AmazonEBSCSIDriverPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEBSCSIDriverPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 04 April 2022, 17:24 UTC
- Waktu telah diedit: 13 Januari 2025, 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEBSCSIDriverPolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshots",
        "ec2:DescribeTags",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot",
```

```
        "ec2:ModifyVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*"
    },
    {
      "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"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/ebs.csi.aws.com/cluster" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "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"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonEC2ContainerRegistryFullAccess

Deskripsi: Menyediakan akses administratif ke sumber daya Amazon ECR

`AmazonEC2ContainerRegistryFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEC2ContainerRegistryFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 21 Desember 2015, 17:06 UTC
- Waktu yang telah diedit: 05 Desember 2020, 00:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryFullAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:*",
        "cloudtrail:LookupEvents"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "replication.ecr.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonEC2ContainerRegistryPowerUser

Deskripsi: Menyediakan akses penuh ke repositori Amazon EC2 Container Registry, tetapi tidak mengizinkan penghapusan repositori atau perubahan kebijakan.

`AmazonEC2ContainerRegistryPowerUser`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEC2ContainerRegistryPowerUser` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 21 Desember 2015, 17:05 UTC
- Waktu yang telah diedit: 10 Desember 2019, 20:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryPowerUser`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:GetRepositoryPolicy",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "ecr:DescribeImages",
        "ecr:BatchGetImage",
        "ecr:GetLifecyclePolicy",
        "ecr:GetLifecyclePolicyPreview",
        "ecr:ListTagsForResource",
        "ecr:DescribeImageScanFindings",
        "ecr:InitiateLayerUpload",
        "ecr:UploadLayerPart",
        "ecr:CompleteLayerUpload",
        "ecr:PutImage"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonEC2ContainerRegistryPullOnly

Deskripsi: Menyediakan akses untuk menarik gambar dari repositori Amazon EC2 Container Registry.

`AmazonEC2ContainerRegistryPullOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEC2ContainerRegistryPullOnly` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 04 Oktober 2024, 16:58 UTC
- Waktu yang telah diedit: 04 Oktober 2024, 16:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryPullOnly`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
        "ecr:GetAuthorizationToken",
        "ecr:BatchGetImage",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchImportUpstreamImage"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonEC2ContainerRegistryReadOnly

Deskripsi: Menyediakan akses hanya-baca ke repositori Amazon EC2 Container Registry.

`AmazonEC2ContainerRegistryReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEC2ContainerRegistryReadOnly` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 21 Desember 2015, 17:04 UTC
- Waktu yang telah diedit: 10 Desember 2019, 20:56 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryReadOnly`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:GetRepositoryPolicy",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "ecr:DescribeImages",
        "ecr:BatchGetImage",
        "ecr:GetLifecyclePolicy",
        "ecr:GetLifecyclePolicyPreview",
        "ecr:ListTagsForResource",
        "ecr:DescribeImageScanFindings"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonEC2ContainerServiceAutoscaleRole

Deskripsi: Kebijakan untuk mengaktifkan Penskalaan Otomatis Tugas untuk Amazon Container Service EC2

`AmazonEC2ContainerServiceAutoscaleRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEC2ContainerServiceAutoscaleRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 12 Mei 2016, 23:25 UTC
- Waktu telah diedit: 05 Februari 2018, 19:15 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceAutoscaleRole`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonEC2ContainerServiceEventsRole

Deskripsi: Kebijakan untuk mengaktifkan CloudWatch Acara untuk Layanan EC2 Kontainer

`AmazonEC2ContainerServiceEventsRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEC2ContainerServiceEventsRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan

- Waktu pembuatan: 30 Mei 2017, 16:51 UTC
- Waktu telah diedit: 06 Maret 2023, 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceEventsRole`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:RunTask"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ecs-tasks.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : "ecs:TagResource",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ecs:CreateAction" : [
            "RunTask"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonEC2ContainerServiceforEC2Role

Deskripsi: Kebijakan default untuk EC2 Peran Amazon untuk Amazon EC2 Container Service.

`AmazonEC2ContainerServiceforEC2Role`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEC2ContainerServiceforEC2Role` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 19 Maret 2015, 18:45 UTC
- Waktu telah diedit: 06 Maret 2023, 22:19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceforEC2Role`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeTags",
        "ecs:CreateCluster",
        "ecs:DeregisterContainerInstance",
        "ecs:DiscoverPollEndpoint",
        "ecs:Poll",
        "ecs:RegisterContainerInstance",
        "ecs:StartTelemetrySession",
        "ecs:UpdateContainerInstancesState",
        "ecs:Submit*",
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ecs:TagResource",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ecs:CreateAction" : [
            "CreateCluster",
            "RegisterContainerInstance"
```

```
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonEC2ContainerServiceRole

Deskripsi: Kebijakan default untuk peran layanan Amazon ECS.

`AmazonEC2ContainerServiceRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEC2ContainerServiceRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 09 April 2015, 16:14 UTC
- Waktu telah diedit: 11 Agustus 2016, 13:08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceRole`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:Describe*",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:Describe*",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:RegisterTargets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonEC2FullAccess

Deskripsi: Menyediakan akses penuh ke Amazon EC2 melalui AWS Management Console.

`AmazonEC2FullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEC2FullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu yang telah diedit: 27 November 2018, 02:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2FullAccess`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : "ec2:*",
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:*",
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : "autoscaling:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "autoscaling.amazonaws.com",
            "ec2scheduled.amazonaws.com",
            "elasticloadbalancing.amazonaws.com",
            "spot.amazonaws.com",
            "spotfleet.amazonaws.com",
            "transitgateway.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonEC2ReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon EC2 melalui AWS Management Console.

`AmazonEC2ReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEC2ReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu yang telah diedit: 27 Desember 2024, 10:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonEC2RoleforAWSCodeDeploy

Deskripsi: Menyediakan EC2 akses ke bucket S3 untuk mengunduh revisi. Peran ini dibutuhkan oleh CodeDeploy agen pada EC2 instance.

`AmazonEC2RoleforAWSCodeDeploy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEC2RoleforAWSCodeDeploy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 19 Mei 2015, 18:10 UTC
- Waktu telah diedit: 20 Maret 2017, 17:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforAWSCodeDeploy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonEC2RoleforAWSCodeDeployLimited

Deskripsi: Menyediakan akses EC2 terbatas ke bucket S3 untuk mengunduh revisi. Peran ini dibutuhkan oleh CodeDeploy agen pada EC2 instance.

`AmazonEC2RoleforAWSCodeDeployLimited`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEC2RoleforAWSCodeDeployLimited` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 24 Agustus 2020, 17:55 UTC
- Waktu telah diedit: 20 Januari 2022 21.37 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforAWSCodeDeployLimited`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::*/CodeDeploy/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
```

```
        "s3:GetObjectVersion"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "s3:ExistingObjectTag/UseWithCodeDeploy" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonEC2RoleforDataPipelineRole

Deskripsi: Kebijakan default untuk EC2 peran layanan Amazon Role for Data Pipeline.

`AmazonEC2RoleforDataPipelineRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEC2RoleforDataPipelineRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu telah diedit: 22 Februari 2016, 17:24 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforDataPipelineRole`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:*",
        "datapipeline:*",
        "dynamodb:*",
        "ec2:Describe*",
        "elasticmapreduce:AddJobFlowSteps",
        "elasticmapreduce:Describe*",
        "elasticmapreduce:ListInstance*",
        "elasticmapreduce:ModifyInstanceGroups",
        "rds:Describe*",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSecurityGroups",
        "s3:*",
        "sdb:*",
        "sns:*",
        "sqs:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonEC2RoleforSSM

Deskripsi: Kebijakan ini akan segera tidak digunakan lagi. Silakan gunakan SSMManaged InstanceCore kebijakan Amazon untuk mengaktifkan fungsionalitas inti layanan AWS Systems Manager pada EC2 instans. Untuk informasi lebih lanjut lihat https://docs.aws.amazon.com/systems-manager/ latest/userguide/setup -instance-profile.html

`AmazonEC2RoleforSSM`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEC2RoleforSSM` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 29 Mei 2015, 17:48 UTC
- Waktu yang telah diedit: 24 Januari 2019, 19:20 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforSSM`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAssociation",
        "ssm:GetDeployablePatchSnapshotForInstance",
        "ssm:GetDocument",
        "ssm:DescribeDocument",
        "ssm:GetManifest",
        "ssm:GetParameters",
        "ssm:ListAssociations",
        "ssm:ListInstanceAssociations",
        "ssm:PutInventory",
        "ssm:PutComplianceItems",
        "ssm:PutConfigurePackageResult",
        "ssm:UpdateAssociationStatus",
        "ssm:UpdateInstanceAssociationStatus",
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2messages:AcknowledgeMessage",
        "ec2messages:DeleteMessage",
        "ec2messages:FailMessage",
        "ec2messages:GetEndpoint",
        "ec2messages:GetMessages",
        "ec2messages:SendReply"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceStatus"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ds:CreateComputer",
        "ds:DescribeDirectories"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:PutObject",
        "s3:GetObject",
        "s3:GetEncryptionConfiguration",
        "s3:AbortMultipartUpload",
        "s3:ListMultipartUploadParts",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonEC2RolePolicyForLaunchWizard

Deskripsi: Kebijakan terkelola untuk peran LaunchWizard layanan Amazon EC2

`AmazonEC2RolePolicyForLaunchWizard`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEC2RolePolicyForLaunchWizard` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 13 November 2019, 08:05 UTC
- Waktu telah diedit: September 25, 2024, 22:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2RolePolicyForLaunchWizard`

Versi kebijakan

Versi kebijakan: v11 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:RebootInstances",
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/LaunchWizardResourceGroupID" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ReplaceRoute"
      ],
      "Resource" : "arn:aws:ec2:*:*:route-table/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/LaunchWizardApplicationType" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAddresses",
        "ec2:AssociateAddress",
        "ec2:DescribeInstances",
        "ec2:DescribeImages",
        "ec2:DescribeRegions",
```

```
        "ec2:DescribeVolumes",
        "ec2:DescribeRouteTables",
        "ec2:ModifyInstanceAttribute",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:PutMetricData",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "LaunchWizardResourceGroupID",
            "LaunchWizardApplicationType"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutObjectTagging",
        "s3:GetBucketLocation",
        "logs:PutLogEvents",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:*",
        "arn:aws:s3:::launchwizard*",
        "arn:aws:s3:::aws-sap-data-provider/config.properties"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : "logs:Create*",
      "Resource" : "arn:aws:logs:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:Describe*",
        "cloudformation:DescribeStackResources",
        "cloudformation:SignalResource",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "LaunchWizardResourceGroupID"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:BatchGetItem",
        "dynamodb:PutItem",
        "sqs:ReceiveMessage",
        "sqs:SendMessage",
        "dynamodb:Scan",
        "s3:ListBucket",
        "dynamodb:Query",
        "dynamodb:UpdateItem",
        "dynamodb:DeleteTable",
        "dynamodb:CreateTable",
        "s3:GetObject",
        "dynamodb:DescribeTable",
        "s3:GetBucketLocation",
        "dynamodb:UpdateTable"
      ],
      "Resource" : [
        "arn:aws:s3:::launchwizard*",
        "arn:aws:dynamodb:*:*:table/LaunchWizard*",
        "arn:aws:sqs:*:*:LaunchWizard*"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ssm:resourceTag/LaunchWizardApplicationType" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:GetDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSSAP-InstallBackint",
        "arn:aws:ssm:*:*:document/AWSSAP-InstallBackintForAWSBackup"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeFileSystems",
        "fsx:ListTagsForResource",
        "fsx:DescribeStorageVirtualMachines"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "LaunchWizard*"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonEC2SpotFleetAutoscaleRole

Deskripsi: Kebijakan untuk mengaktifkan Penskalaan Otomatis untuk Armada Spot Amazon EC2

`AmazonEC2SpotFleetAutoscaleRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEC2SpotFleetAutoscaleRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 19 Agustus 2016, 18:27 UTC
- Waktu yang telah diedit: 18 Februari 2019, 19:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2SpotFleetAutoscaleRole`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      "Action" : [
        "ec2:DescribeSpotFleetRequests",
        "ec2:ModifySpotFleetRequest"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/ec2.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_EC2SpotFleetRequest",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "ec2.application-autoscaling.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonEC2SpotFleetTaggingRole

Deskripsi: Memungkinkan Armada EC2 Spot untuk meminta, menghentikan, dan menandai Instans Spot atas nama Anda.

`AmazonEC2SpotFleetTaggingRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEC2SpotFleetTaggingRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 29 Juni 2017, 18:19 UTC
- Waktu yang telah diedit: 23 April 2020, 19:30 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2SpotFleetTaggingRole`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSubnets",
        "ec2:RequestSpotInstances",
        "ec2:TerminateInstances",
        "ec2:DescribeInstanceStatus",
```

```
        "ec2:CreateTags",
        "ec2:RunInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      },
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterTargets"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:*/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonECS_FullAccess

Deskripsi: Menyediakan akses administratif ke sumber daya Amazon ECS dan mengaktifkan fitur ECS melalui akses ke sumber daya AWS layanan lain, termasuk grup Auto Scaling VPCs, dan tumpukan. CloudFormation

`AmazonECS_FullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonECS_FullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 07 November 2017, 21:36 UTC
- Waktu telah diedit: 13 Agustus 2024, 19:39 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonECS_FullAccess`

Versi kebijakan

Versi kebijakan: v21 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonECSComputeServiceRolePolicy

Deskripsi: Kebijakan untuk mengaktifkan Amazon ECS Compute mengelola EC2 instans dan sumber daya terkait sebagai bagian dari instans yang dikelola ECS

`AmazonECSComputeServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 24 Maret 2025, 17:37 UTC
- Waktu yang telah diedit: 28 Maret 2025, 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonECSComputeServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerS

Deskripsi: Menyediakan akses administratif ke Private Certificate Authority, AWS Secrets Manager, dan lainnya yang Layanan AWS diperlukan untuk mengelola fitur ECS Service Connect TLS atas nama Anda.

`AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 19 Januari 2024, 20:08 UTC
- Waktu telah diedit: 19 Januari 2024, 20:08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateSecret",
      "Effect" : "Allow",
      "Action" : "secretsmanager:CreateSecret",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:ecs-sc!*",
      "Condition" : {
        "ArnLike" : {
          "aws:RequestTag/AmazonECSCreated" : [
            "arn:aws:ecs:*:*:service/*/*",
            "arn:aws:ecs:*:*:task-set/*/*"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagOnCreateSecret",
      "Effect" : "Allow",
      "Action" : "secretsmanager:TagResource",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:ecs-sc!*",
      "Condition" : {
        "ArnLike" : {
          "aws:RequestTag/AmazonECSCreated" : [
            "arn:aws:ecs:*:*:service/*/*",
            "arn:aws:ecs:*:*:task-set/*/*"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "RotateTLSCertificateSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue",
        "secretsmanager:DeleteSecret",
        "secretsmanager:RotateSecret",
        "secretsmanager:UpdateSecretVersionStage"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:ecs-sc!*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "ecs-sc",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ManagePrivateCertificateAuthority",
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:GetCertificate",
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:DescribeCertificateAuthority"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "ManagePrivateCertificateAuthorityForIssuingEndEntityCertificate",
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true",
          "acm-pca:TemplateArn" : "arn:aws:acm-pca:::template/EndEntityCertificate/V1"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonECSInfrastructureRolePolicyForVolumes

Deskripsi: Menyediakan akses ke sumber daya AWS layanan lain yang diperlukan untuk mengelola volume yang terkait dengan beban kerja ECS atas nama Anda.

`AmazonECSInfrastructureRolePolicyForVolumes`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonECSInfrastructureRolePolicyForVolumes` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 10 Januari 2024, 22:56 UTC
- Waktu yang telah diedit: 28 Mei 2025, 20:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonECSInfrastructureRolePolicyForVolumes`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateEBSManagedVolume",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVolume",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "ArnLike" : {
          "aws:RequestTag/AmazonECSCreated" : "arn:aws:ecs:*:*:task/*"
        },
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "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"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonECSInfrastructureRolePolicyForVpcLattice

Deskripsi: Menyediakan akses ke sumber daya AWS layanan lain yang diperlukan untuk mengelola fitur VPC Lattice di beban kerja ECS atas nama Anda.

`AmazonECSInfrastructureRolePolicyForVpcLattice`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonECSInfrastructureRolePolicyForVpcLattice` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 15 November 2024, 20:02 UTC
- Waktu telah diedit: November 15, 2024, 20:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonECSInfrastructureRolePolicyForVpcLattice`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonECSServiceRolePolicy

Deskripsi: Kebijakan untuk mengaktifkan Amazon ECS mengelola klaster Anda.

`AmazonECSServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 14 Oktober 2017, 01:18 UTC
- Waktu yang telah diedit: 24 Juni 2025, 21:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonECSServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v12 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ECSTaskManagement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachNetworkInterface",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:Describe*",
        "ec2:DetachNetworkInterface",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:Describe*",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:RegisterTargets",
        "route53:ChangeResourceRecordSets",
        "route53:CreateHealthCheck",
        "route53:DeleteHealthCheck",
        "route53:Get*",
```

```
        "route53:List*",
        "route53:UpdateHealthCheck",
        "servicediscovery:DeregisterInstance",
        "servicediscovery:Get*",
        "servicediscovery:List*",
        "servicediscovery:RegisterInstance",
        "servicediscovery:UpdateInstanceCustomHealthStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AutoScaling",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AutoScalingManagement",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DeletePolicy",
        "autoscaling:PutScalingPolicy",
        "autoscaling:SetInstanceProtection",
        "autoscaling:UpdateAutoScalingGroup",
        "autoscaling:PutLifecycleHook",
        "autoscaling:DeleteLifecycleHook",
        "autoscaling:CompleteLifecycleAction",
        "autoscaling:RecordLifecycleActionHeartbeat"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "autoscaling:ResourceTag/AmazonECSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "AutoScalingPlanManagement",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling-plans:CreateScalingPlan",
        "autoscaling-plans:DeleteScalingPlan",
```

```
        "autoscaling-plans:DescribeScalingPlans",
        "autoscaling-plans:DescribeScalingPlanResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EventBridge",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/ecs-managed-*"
    },
    {
      "Sid" : "EventBridgeRuleManagement",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "ecs.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CWAlarmManagement",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:*"
    },
    {
      "Sid" : "ECSTagging",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
```

```
      "Resource" : "arn:aws:ec2:*:*:network-interface/*"
    },
    {
      "Sid" : "CWLogGroupManagement",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/ecs/*"
    },
    {
      "Sid" : "CWLogStreamManagement",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/ecs/*:log-stream:*"
    },
    {
      "Sid" : "ExecuteCommandSessionManagement",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeSessions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ExecuteCommand",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:task/*",
        "arn:aws:ssm:*:*:document/AmazonECS-ExecuteInteractiveCommand"
      ]
    },
    {
      "Sid" : "CloudMapResourceCreation",
      "Effect" : "Allow",
```

```
      "Action" : [
        "servicediscovery:CreateHttpNamespace",
        "servicediscovery:CreateService"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonECSManaged"
          ]
        }
      }
    },
    {
      "Sid" : "CloudMapResourceTagging",
      "Effect" : "Allow",
      "Action" : "servicediscovery:TagResource",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AmazonECSManaged" : "*"
        }
      }
    },
    {
      "Sid" : "CloudMapResourceDeletion",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DeleteService"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonECSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "CloudMapResourceDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DiscoverInstances",
        "servicediscovery:DiscoverInstancesRevision"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "CloudMapResourceAttributeManagement",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:UpdateServiceAttributes"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonECSManaged" : "false"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonECSTaskExecutionRolePolicy

Deskripsi: Menyediakan akses ke sumber daya AWS layanan lain yang diperlukan untuk menjalankan tugas Amazon ECS

`AmazonECSTaskExecutionRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonECSTaskExecutionRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 16 November 2017, 18:48 UTC

- Waktu telah diedit: 16 November 2017, 18:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonECSTaskExecutionRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonEFSCSIDriverPolicy

Deskripsi: Menyediakan akses manajemen ke sumber daya EFS dan akses baca EC2

`AmazonEFSCSIDriverPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEFSCSIDriverPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 25 Juli 2023, 20:10 UTC
- Waktu telah diedit: 25 Juli 2023, 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEFSCSIDriverPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowDescribe",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "AllowCreateAccessPoint",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:CreateAccessPoint"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/efs.csi.aws.com/cluster" : "false"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "efs.csi.aws.com/cluster"
        }
      }
    },
    {
      "Sid" : "AllowTagNewAccessPoints",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "elasticfilesystem:CreateAction" : "CreateAccessPoint"
        },
        "Null" : {
          "aws:RequestTag/efs.csi.aws.com/cluster" : "false"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "efs.csi.aws.com/cluster"
        }
      }
    },
    {
      "Sid" : "AllowDeleteAccessPoint",
      "Effect" : "Allow",
      "Action" : "elasticfilesystem:DeleteAccessPoint",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/efs.csi.aws.com/cluster" : "false"
```

```
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonEKS_CNI_Policy

Deskripsi: Kebijakan ini memberikan izin kepada Amazon VPC CNI Plugin (amazon-vpc-cni-k8s) yang diperlukan untuk mengubah konfigurasi alamat IP pada node pekerja EKS Anda. Set izin ini memungkinkan CNI untuk membuat daftar, mendeskripsikan, dan memodifikasi Antarmuka Jaringan Elastis atas nama Anda. Informasi lebih lanjut tentang Plugin AWS VPC CNI tersedia di sini: 8s https://github.com/aws/ amazon-vpc-cni-k

`AmazonEKS_CNI_Policy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEKS_CNI_Policy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Mei 2018, 21:07 UTC
- Waktu telah diedit: 04 Maret 2024, 20:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKS_CNI_Policy`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonEKSCNIPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignPrivateIpAddresses",
        "ec2:AttachNetworkInterface",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeInstances",
        "ec2:DescribeTags",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeSubnets",
        "ec2:DetachNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonEKSCNIPolicyENITag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonEKSBlockStoragePolicy

Deskripsi: Kebijakan yang dilampirkan pada Peran Kluster EKS yang memberikan izin untuk mengelola sumber daya penyimpanan blok klaster.

`AmazonEKSBlockStoragePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEKSBlockStoragePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 Oktober 2024, 20:18 UTC
- Waktu telah diedit: 30 Oktober 2024, 20:18 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSBlockStoragePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "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"
          ]
        }
```

```
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonEKSClusterPolicy

Deskripsi: Kebijakan ini memberi Kubernetes izin yang diperlukan untuk mengelola sumber daya atas nama Anda. Kubernetes memerlukan CreateTags izin Ec2: untuk menempatkan informasi identifikasi pada EC2 sumber daya termasuk namun tidak terbatas pada Instans, Grup Keamanan, dan Antarmuka Jaringan Elastis.

`AmazonEKSClusterPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEKSClusterPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Mei 2018, 21:06 UTC
- Waktu telah diedit: 17 April 2025, 02:52 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSClusterPolicy`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonEKSComputePolicy

Deskripsi: Kebijakan yang dilampirkan pada Peran Kluster EKS yang memberikan izin untuk mengelola sumber daya komputasi klaster.

`AmazonEKSComputePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEKSComputePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 November 2024, 21:46 UTC
- Waktu yang telah diedit: 20 Juni 2025, 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSComputePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonEKSConnectorServiceRolePolicy

Deskripsi: Kebijakan ini memungkinkan Amazon EKS mengelola AWS sumber daya untuk konektor EKS

`AmazonEKSConnectorServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 04 September 2021 20:31 UTC
- Waktu yang telah diedit: 04 September 2021, 20:31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSConnectorServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
        "ssm:DescribeInstanceInformation",
        "ssm:DeleteActivation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConnectorAgentStartSession",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
        "arn:aws:eks:*:*:cluster/*",
        "arn:aws:ssm:*::document/AmazonEKS-ExecuteNonInteractiveCommand"
      ]
    },
    {
      "Sid" : "ConnectorAgentDeregister",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeregisterManagedInstance"
      ],
      "Resource" : [
        "arn:aws:eks:*:*:cluster/*"
      ]
    },
    {
      "Sid" : "PassAnyRoleToSsm",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PutManagedEventRule",
      "Effect" : "Allow",
```

```
      "Action" : "events:PutRule",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "eks-connector.amazonaws.com",
          "events:source" : "aws.ssm"
        }
      }
    },
    {
      "Sid" : "PutManagedEventTarget",
      "Effect" : "Allow",
      "Action" : "events:PutTargets",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "eks-connector.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonEKSDashboardConsoleReadOnly

Deskripsi: Menyediakan akses baca saja untuk melihat dasbor di konsol Amazon EKS. Dasbor mengumpulkan informasi tentang beberapa cluster dan sumber daya terkait menggunakan Organizations AWS .

`AmazonEKSDashboardConsoleReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEKSDashboardConsoleReadOnly` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 19 Juni 2025, 17:22 UTC
- Waktu yang telah diedit: 19 Juni 2025, 17:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSDashboardConsoleReadOnly`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonEKSDashboardServiceRolePolicy

Deskripsi: Kebijakan ini memungkinkan Dasbor Amazon EKS mengakses dan menampilkan informasi di seluruh organisasi. Kebijakan ini memungkinkan layanan Dasbor EKS untuk mengumpulkan informasi tentang struktur dan akun AWS Organisasi Anda.

`AmazonEKSDashboardServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 08 Mei 2025, 19:07 UTC
- Waktu yang telah diedit: Mei 08, 2025, 19:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSDashboardServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonEKSFargatePodExecutionRolePolicy

Deskripsi: Menyediakan akses ke sumber daya AWS layanan lain yang diperlukan untuk menjalankan pod Amazon EKS di AWS Fargate

`AmazonEKSFargatePodExecutionRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEKSFargatePodExecutionRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 22 November 2019, 04:34 UTC
- Waktu telah diedit: 22 November 2019, 04:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSFargatePodExecutionRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonEKSForFargateServiceRolePolicy

Deskripsi: Kebijakan ini memberikan izin yang diperlukan ke Amazon EKS untuk menjalankan tugas fargate

`AmazonEKSForFargateServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 22 November 2019, 04:36 UTC

- Waktu telah diedit: 22 November 2019, 04:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSForFargateServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonEKSLoadBalancingPolicy

Deskripsi: Kebijakan yang dilampirkan pada Peran Kluster EKS yang memberikan izin untuk mengelola sumber daya penyeimbang beban klaster.

`AmazonEKSLoadBalancingPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEKSLoadBalancingPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 Oktober 2024, 20:18 UTC
- Waktu telah diedit: 09 Januari 2025, 22:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSLoadBalancingPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonEKSLocalOutpostClusterPolicy

Deskripsi: Kebijakan ini memberikan izin ke instans bidang kontrol kluster lokal EKS yang berjalan di akun Anda untuk mengelola sumber daya atas nama Anda.

`AmazonEKSLocalOutpostClusterPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEKSLocalOutpostClusterPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 24 Agustus 2022 21:56 UTC
- Waktu yang telah diedit: 24 Oktober 2024, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSLocalOutpostClusterPolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonEKSLocalOutpostServiceRolePolicy

Deskripsi: Memungkinkan Amazon EKS Lokal untuk memanggil AWS layanan atas nama Anda.

`AmazonEKSLocalOutpostServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 23 Agustus 2022, 21:53 UTC
- Waktu yang telah diedit: 26 Juni 2025, 18:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSLocalOutpostServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeRouteTables",
        "ec2:DescribeAddresses",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribePlacementGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/eks-local:controlplane-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/eks-local:controlplane-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "StringLike" : {
```

```
          "aws:RequestTag/eks-local:controlplane-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/eks-local:controlplane-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:placement-group/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:TerminateInstances",
        "ec2:GetConsoleOutput"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/eks-local:controlplane-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "kubernetes.io/cluster/*",
            "eks*"
          ]
        },
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateNetworkInterface",
            "CreateSecurityGroup",
            "RunInstances"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:eks-local.cluster.x-k8s.io/*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "kubernetes.io/cluster/*",
            "eks*"
          ]
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:eks-local.cluster.x-k8s.io/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/eks-local:controlplane-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "secretsmanager:DeleteSecret",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:eks-local.cluster.x-k8s.io/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/eks-local:controlplane-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "secretsmanager:DescribeSecret",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:eks-local.cluster.x-k8s.io/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "iam:GetInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile"
      ],
      "Resource" : "arn:aws:iam::*:instance-profile/eks-local-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ssm:resourceTag/eks-local:controlplane-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : "arn:aws:ssm:*::document/AmazonEKS-ControlPlaneInstanceProxy"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "arn:aws:ssm:*:*:session/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:ResumeSession",
        "ssm:TerminateSession"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "outposts:GetOutpost"
```

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonEKSNetworkingPolicy

Deskripsi: Kebijakan yang dilampirkan pada Peran Kluster EKS yang memberikan izin untuk mengelola sumber daya jaringan klaster.

`AmazonEKSNetworkingPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEKSNetworkingPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 Oktober 2024, 22:34 UTC
- Waktu telah diedit: 28 Oktober 2024, 22:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSNetworkingPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonEKSServicePolicy

Deskripsi: Kebijakan ini memungkinkan Amazon Elastic Container Service for Kubernetes untuk membuat dan mengelola sumber daya yang diperlukan untuk mengoperasikan EKS Cluster.

`AmazonEKSServicePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEKSServicePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Mei 2018, 21:08 UTC
- Waktu yang telah diedit: 14 Oktober 2024, 21:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSServicePolicy`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DetachNetworkInterface",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:ModifyNetworkInterfaceAttribute",
        "iam:ListAttachedRolePolicies",
        "eks:UpdateClusterVersion",
        "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"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonEKSServiceRolePolicy

Deskripsi: Peran Tertaut Layanan yang diperlukan Amazon EKS untuk menelepon AWS layanan atas nama Anda.

`AmazonEKSServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan

- Waktu pembuatan: 21 Februari 2020, 20:10 UTC
- Waktu yang telah diedit: 20 Juni 2025, 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonEKSVPCResourceController

Deskripsi: Kebijakan yang digunakan oleh VPC Resource Controller untuk mengelola ENI dan IPs untuk node pekerja.

`AmazonEKSVPCResourceController`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEKSVPCResourceController` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 12 Agustus 2020 00:55 UTC
- Waktu yang telah diedit: 12 Agustus 2020, 00:55 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSVPCResourceController`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterfacePermission",
      "Resource" : "*",
      "Condition" : {
```

```
        "ForAnyValue:StringEquals" : {
          "ec2:ResourceTag/eks:eni:owner" : "eks-vpc-resource-controller"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DetachNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface",
        "ec2:AttachNetworkInterface",
        "ec2:UnassignPrivateIpAddresses",
        "ec2:AssignPrivateIpAddresses"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonEKSWorkerNodeMinimalPolicy

Deskripsi: Kebijakan ini memungkinkan node pekerja Amazon EKS terhubung ke Amazon EKS Cluster.

`AmazonEKSWorkerNodeMinimalPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEKSWorkerNodeMinimalPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 02 Oktober 2024, 20:03 UTC
- Waktu yang telah diedit: 02 Oktober 2024, 20:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSWorkerNodeMinimalPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "WorkerNodePermissions",
      "Effect" : "Allow",
      "Action" : [
        "eks-auth:AssumeRoleForPodIdentity"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonEKSWorkerNodePolicy

Deskripsi: Kebijakan ini memungkinkan node pekerja Amazon EKS terhubung ke Amazon EKS Cluster.

`AmazonEKSWorkerNodePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEKSWorkerNodePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Mei 2018, 21:09 UTC
- Waktu yang telah diedit: 27 November 2023, 00:06 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSWorkerNodePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "WorkerNodePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
```

```
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeVpcs",
        "eks:DescribeCluster",
        "eks-auth:AssumeRoleForPodIdentity"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonElastiCacheFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon ElastiCache melalui AWS Management Console.

`AmazonElastiCacheFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonElastiCacheFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu telah diedit: 28 November 2023, 03:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElastiCacheFullAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonElastiCacheReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon ElastiCache melalui AWS Management Console.

`AmazonElastiCacheReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonElastiCacheReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu telah diedit: 06 Februari 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElastiCacheReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonElasticContainerRegistryPublicFullAccess

Deskripsi: Menyediakan akses administratif ke sumber daya Publik Amazon ECR

`AmazonElasticContainerRegistryPublicFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonElasticContainerRegistryPublicFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Desember 2020, 17:25 UTC
- Waktu yang telah diedit: 01 Desember 2020, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticContainerRegistryPublicFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonElasticContainerRegistryPublicPowerUser

Deskripsi: Menyediakan akses penuh ke repositori Publik Amazon ECR, tetapi tidak mengizinkan penghapusan repositori atau perubahan kebijakan.

`AmazonElasticContainerRegistryPublicPowerUser`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonElasticContainerRegistryPublicPowerUser` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Desember 2020, 16:16 UTC
- Waktu yang telah diedit: 01 Desember 2020, 16:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticContainerRegistryPublicPowerUser`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr-public:GetAuthorizationToken",
        "sts:GetServiceBearerToken",
        "ecr-public:BatchCheckLayerAvailability",
        "ecr-public:GetRepositoryPolicy",
        "ecr-public:DescribeRepositories",
        "ecr-public:DescribeRegistries",
        "ecr-public:DescribeImages",
        "ecr-public:DescribeImageTags",
        "ecr-public:GetRepositoryCatalogData",
        "ecr-public:GetRegistryCatalogData",
        "ecr-public:InitiateLayerUpload",
        "ecr-public:UploadLayerPart",
        "ecr-public:CompleteLayerUpload",
        "ecr-public:PutImage"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonElasticContainerRegistryPublicReadOnly

Deskripsi: Menyediakan akses hanya-baca ke repositori Publik Amazon ECR.

`AmazonElasticContainerRegistryPublicReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonElasticContainerRegistryPublicReadOnly` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Desember 2020, 17:27 UTC
- Waktu yang telah diedit: 01 Desember 2020, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticContainerRegistryPublicReadOnly`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr-public:GetAuthorizationToken",
        "sts:GetServiceBearerToken",
        "ecr-public:BatchCheckLayerAvailability",
        "ecr-public:GetRepositoryPolicy",
        "ecr-public:DescribeRepositories",
        "ecr-public:DescribeRegistries",
        "ecr-public:DescribeImages",
        "ecr-public:DescribeImageTags",
        "ecr-public:GetRepositoryCatalogData",
        "ecr-public:GetRegistryCatalogData"
      ],
```

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonElasticFileSystemClientFullAccess

Deskripsi: Menyediakan akses klien root ke sistem file Amazon EFS

`AmazonElasticFileSystemClientFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonElasticFileSystemClientFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 13 Januari 2020, 16:27 UTC
- Waktu yang telah diedit: 13 Januari 2020, 16:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemClientFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:ClientMount",
        "elasticfilesystem:ClientRootAccess",
        "elasticfilesystem:ClientWrite",
        "elasticfilesystem:DescribeMountTargets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonElasticFileSystemClientReadOnlyAccess

Deskripsi: Menyediakan akses klien hanya baca ke sistem file Amazon EFS

`AmazonElasticFileSystemClientReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonElasticFileSystemClientReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 13 Januari 2020, 16:24 UTC
- Waktu yang telah diedit: 13 Januari 2020, 16:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemClientReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonElasticFileSystemClientReadWriteAccess

Deskripsi: Menyediakan akses klien baca dan tulis ke sistem file Amazon EFS

`AmazonElasticFileSystemClientReadWriteAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonElasticFileSystemClientReadWriteAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 13 Januari 2020, 16:21 UTC
- Waktu yang telah diedit: 13 Januari 2020, 16:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemClientReadWriteAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonElasticFileSystemFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon EFS melalui AWS Management Console.

`AmazonElasticFileSystemFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonElasticFileSystemFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Mei 2015, 16:22 UTC
- Waktu telah diedit: 07 November 2024, 19:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemFullAccess`

Versi kebijakan

Versi kebijakan: v10 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonElasticFileSystemReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon EFS melalui AWS Management Console.

`AmazonElasticFileSystemReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonElasticFileSystemReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Mei 2015, 16:25 UTC
- Waktu telah diedit: 07 November 2024, 19:39 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonElasticFileSystemServiceRolePolicy

Deskripsi: Memungkinkan Amazon Elastic File System mengelola AWS sumber daya atas nama Anda

`AmazonElasticFileSystemServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 05 November 2019, 16:52 UTC
- Waktu telah diedit: 07 November 2024, 19:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonElasticFileSystemServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "backup-storage:MountCapsule",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:ModifyNetworkInterfaceAttribute",
        "tag:GetResources"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "backup:CreateBackupVault",
        "backup:PutBackupVaultAccessPolicy"
      ],
      "Resource" : [
        "arn:aws:backup:*:*:backup-vault:aws/efs/automatic-backup-vault"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "backup:CreateBackupPlan",
        "backup:CreateBackupSelection"
      ],
      "Resource" : [
        "arn:aws:backup:*:*:backup-plan:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "backup.amazonaws.com"
          ]
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/backup.amazonaws.com/
AWSServiceRoleForBackup"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "backup.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:CreateReplicationConfiguration",
        "elasticfilesystem:DescribeReplicationConfigurations",
        "elasticfilesystem:DeleteReplicationConfiguration",
        "elasticfilesystem:ReplicationRead",
        "elasticfilesystem:ReplicationWrite"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonElasticFileSystemsUtils

Deskripsi: Memungkinkan pelanggan menggunakan AWS Systems Manager untuk secara otomatis mengelola paket Amazon EFS utilities (amazon-efs-utils) pada EC2 instans mereka, dan menggunakannya CloudWatchLog untuk mendapatkan notifikasi keberhasilan/kegagalan pemasangan sistem file EFS.

`AmazonElasticFileSystemsUtils`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonElasticFileSystemsUtils` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 September 2020, 15:16 UTC
- Waktu yang telah diedit: 29 September 2020, 15:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemsUtils`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAssociation",
        "ssm:GetDeployablePatchSnapshotForInstance",
        "ssm:GetDocument",
        "ssm:DescribeDocument",
        "ssm:GetManifest",
        "ssm:GetParameter",
        "ssm:GetParameters",
        "ssm:ListAssociations",
        "ssm:ListInstanceAssociations",
        "ssm:PutInventory",
```

```
        "ssm:PutComplianceItems",
        "ssm:PutConfigurePackageResult",
        "ssm:UpdateAssociationStatus",
        "ssm:UpdateInstanceAssociationStatus",
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2messages:AcknowledgeMessage",
        "ec2messages:DeleteMessage",
        "ec2messages:FailMessage",
        "ec2messages:GetEndpoint",
        "ec2messages:GetMessages",
        "ec2messages:SendReply"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeMountTargets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents",
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups",
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonElasticMapReduceEditorsRole

Deskripsi: Kebijakan default untuk peran layanan Amazon Elastic MapReduce Editors.

`AmazonElasticMapReduceEditorsRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonElasticMapReduceEditorsRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 16 November 2018, 21:55 UTC
- Waktu telah diedit: 09 Februari 2023, 22:39 UTC

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

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeNetworkInterfaces",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeTags",
        "ec2:DescribeInstances",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:ListSteps"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws:elasticmapreduce:editor-id",
            "aws:elasticmapreduce:job-flow-id"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonElasticMapReduceforAutoScalingRole

Deskripsi: Amazon Elastic MapReduce untuk Auto Scaling. Peran untuk memungkinkan Auto Scaling menambah dan menghapus instance dari kluster EMR Anda.

`AmazonElasticMapReduceforAutoScalingRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonElasticMapReduceforAutoScalingRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 18 November 2016, 01:09 UTC
- Waktu telah diedit: 18 November 2016, 01:09 UTC

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

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ModifyInstanceGroups"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonElasticMapReduceforEC2Role

Deskripsi: Kebijakan default untuk Amazon Elastic MapReduce untuk peran EC2 layanan.

`AmazonElasticMapReduceforEC2Role`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonElasticMapReduceforEC2Role` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu telah diedit: 11 Agustus 2017, 23:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceforEC2Role`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "cloudwatch:*",
        "dynamodb:*",
        "ec2:Describe*",
        "elasticmapreduce:Describe*",
        "elasticmapreduce:ListBootstrapActions",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListInstances",
```

```
        "elasticmapreduce:ListSteps",
        "kinesis:CreateStream",
        "kinesis:DeleteStream",
        "kinesis:DescribeStream",
        "kinesis:GetRecords",
        "kinesis:GetShardIterator",
        "kinesis:MergeShards",
        "kinesis:PutRecord",
        "kinesis:SplitShard",
        "rds:Describe*",
        "s3:*",
        "sdb:*",
        "sns:*",
        "sqs:*",
        "glue:CreateDatabase",
        "glue:UpdateDatabase",
        "glue:DeleteDatabase",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:CreateTable",
        "glue:UpdateTable",
        "glue:DeleteTable",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetTableVersions",
        "glue:CreatePartition",
        "glue:BatchCreatePartition",
        "glue:UpdatePartition",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:BatchGetPartition",
        "glue:CreateUserDefinedFunction",
        "glue:UpdateUserDefinedFunction",
        "glue:DeleteUserDefinedFunction",
        "glue:GetUserDefinedFunction",
        "glue:GetUserDefinedFunctions"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonElasticMapReduceFullAccess

Deskripsi: Kebijakan ini berada di jalur penghentian. Lihat dokumentasi untuk panduan: https:// docs.aws.amazon.com/emr/ latest/ManagementGuide/emr - managed-iam-policies .html. Menyediakan akses penuh ke Amazon Elastic MapReduce dan layanan dasar yang diperlukan seperti EC2 dan S3

`AmazonElasticMapReduceFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonElasticMapReduceFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu yang telah diedit: 11 Oktober 2019, 15:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticMapReduceFullAccess`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudwatch:*",
        "cloudformation:CreateStack",
        "cloudformation:DescribeStackEvents",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:CancelSpotInstanceRequests",
        "ec2:CreateRoute",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags",
        "ec2:DeleteRoute",
        "ec2:DeleteTags",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSpotPriceHistory",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:DescribeRouteTables",
        "ec2:DescribeNetworkAcls",
        "ec2:CreateVpcEndpoint",
        "ec2:ModifyImageAttribute",
        "ec2:ModifyInstanceAttribute",
        "ec2:RequestSpotInstances",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RunInstances",
        "ec2:TerminateInstances",
        "elasticmapreduce:*",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:ListRoles",
```

```
        "iam:PassRole",
        "kms:List*",
        "s3:*",
        "sdb:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : [
            "elasticmapreduce.amazonaws.com",
            "elasticmapreduce.amazonaws.com.cn"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonElasticMapReducePlacementGroupPolicy

Deskripsi: Kebijakan untuk mengizinkan EMR membuat, mendeskripsikan, dan menghapus grup EC2 penempatan.

`AmazonElasticMapReducePlacementGroupPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonElasticMapReducePlacementGroupPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 September 2020 00:37 UTC
- Waktu yang telah diedit: 29 September 2020, 00:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticMapReducePlacementGroupPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Resource" : "*",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeletePlacementGroup",
        "ec2:DescribePlacementGroups"
      ]
    },
    {
      "Resource" : "arn:aws:ec2:*:*:placement-group/EMR_*",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreatePlacementGroup"
      ]
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonElasticMapReduceReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon Elastic MapReduce melalui AWS Management Console.

`AmazonElasticMapReduceReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonElasticMapReduceReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu yang telah diedit: 29 Juli 2020, 23:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticMapReduceReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elasticmapreduce:Describe*",
        "elasticmapreduce:List*",
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:ViewEventsFromAllClustersInConsole",
        "s3:GetObject",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "sdb:Select",
        "cloudwatch:GetMetricStatistics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonElasticMapReduceRole

Deskripsi: Kebijakan ini berada di jalur penghentian. Lihat dokumentasi untuk panduan: https:// docs.aws.amazon.com/emr/ latest/ManagementGuide/emr - managed-iam-policies .html. Kebijakan default untuk peran MapReduce layanan Amazon Elastic.

`AmazonElasticMapReduceRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonElasticMapReduceRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu yang telah diedit: 24 Juni 2020, 22:24 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceRole`

Versi kebijakan

Versi kebijakan: v10 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CancelSpotInstanceRequests",
        "ec2:CreateFleet",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteTags",
```

```
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSpotPriceHistory",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeVpcs",
        "ec2:DetachNetworkInterface",
        "ec2:ModifyImageAttribute",
        "ec2:ModifyInstanceAttribute",
        "ec2:RequestSpotInstances",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RunInstances",
        "ec2:TerminateInstances",
        "ec2:DeleteVolume",
        "ec2:DescribeVolumeStatus",
        "ec2:DescribeVolumes",
        "ec2:DetachVolume",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListInstanceProfiles",
        "iam:ListRolePolicies",
        "iam:PassRole",
        "s3:CreateBucket",
        "s3:Get*",
        "s3:List*",
        "sdb:BatchPutAttributes",
        "sdb:Select",
        "sqs:CreateQueue",
        "sqs:Delete*",
```

```
        "sqs:GetQueue*",
        "sqs:PurgeQueue",
        "sqs:ReceiveMessage",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms",
        "application-autoscaling:RegisterScalableTarget",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:Describe*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/spot.amazonaws.com/
AWSServiceRoleForEC2Spot*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "spot.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonElasticsearchServiceRolePolicy

Deskripsi: Izinkan Amazon Elasticsearch Service mengakses AWS layanan lain seperti EC2 Jaringan APIs atas nama Anda.

`AmazonElasticsearchServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 07 Juli 2017, 00:15 UTC
- Waktu telah diedit: 23 Oktober 2023, 06:58 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonElasticsearchServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Stmt1480452973134",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:AddListenerCertificates",
        "elasticloadbalancing:RemoveListenerCertificates"
      ],
```

```
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973135",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973136",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/ES"
        }
      }
    },
    {
      "Sid" : "Stmt1480452973198",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*"
      ]
    },
    {
      "Sid" : "Stmt1480452973199",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/OpenSearchManaged" : "true"
```

```
        }
      }
    },
    {
      "Sid" : "Stmt1480452973200",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint",
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/OpenSearchManaged" : "true"
        }
      }
    },
    {
      "Sid" : "Stmt1480452973201",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973149",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignIpv6Addresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*"
    },
    {
      "Sid" : "Stmt1480452973150",
      "Effect" : "Allow",
      "Action" : [
        "ec2:UnAssignIpv6Addresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*"
    },
    {
      "Sid" : "Stmt1480452973202",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonElasticTranscoder_FullAccess

Deskripsi: Memberikan pengguna akses penuh ke Elastic Transcoder dan akses ke layanan terkait yang diperlukan untuk fungsionalitas Elastic Transcoder penuh.

`AmazonElasticTranscoder_FullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonElasticTranscoder_FullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 April 2018, 18:59 UTC
- Waktu yang telah diedit: 10 Juni 2019, 22:51 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticTranscoder_FullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elastictranscoder:*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "iam:ListRoles",
        "sns:ListTopics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "elastictranscoder.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonElasticTranscoder_JobsSubmitter

Deskripsi: Memberikan izin kepada pengguna untuk mengubah preset, mengirimkan pekerjaan, dan melihat setelan Elastic Transcoder. Kebijakan ini juga memberikan beberapa akses hanya-baca ke beberapa layanan lain yang diperlukan untuk menggunakan konsol Transcode Elastic, termasuk S3, IAM, dan SNS.

`AmazonElasticTranscoder_JobsSubmitter`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonElasticTranscoder_JobsSubmitter` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 07 Juni 2018, 21:12 UTC
- Waktu yang telah diedit: 10 Juni 2019, 22:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticTranscoder_JobsSubmitter`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elastictranscoder:Read*",
        "elastictranscoder:List*",
        "elastictranscoder:*Job",
        "elastictranscoder:*Preset",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "iam:ListRoles",
        "sns:ListTopics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonElasticTranscoder_ReadOnlyAccess

Deskripsi: Memberikan pengguna akses hanya-baca ke Elastic Transcoder dan daftar akses ke layanan terkait.

`AmazonElasticTranscoder_ReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonElasticTranscoder_ReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 07 Juni 2018, 21:09 UTC
- Waktu yang telah diedit: 10 Juni 2019, 22:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticTranscoder_ReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elastictranscoder:Read*",
        "elastictranscoder:List*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "iam:ListRoles",
        "sns:ListTopics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonElasticTranscoderRole

Deskripsi: Kebijakan default untuk peran layanan Amazon Elastic Transcoder.

`AmazonElasticTranscoderRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonElasticTranscoderRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu yang telah diedit: 13 Juni 2019, 22:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticTranscoderRole`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:Get*",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:*MultipartUpload*"
      ],
      "Sid" : "1",
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Sid" : "2",
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonEMRCleanupPolicy

Deskripsi: Memungkinkan tindakan yang diperlukan EMR untuk menghentikan dan menghapus AWS EC2 sumber daya jika peran Layanan EMR telah kehilangan kemampuan itu.

`AmazonEMRCleanupPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 26 September 2017, 23:54 UTC
- Waktu yang telah diedit: 29 September 2020, 21:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEMRCleanupPolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonEMRContainersServiceRolePolicy

Deskripsi: Memungkinkan akses ke sumber daya AWS layanan lain yang diperlukan untuk menjalankan Amazon EMR

`AmazonEMRContainersServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 09 Desember 2020, 00:38 UTC
- Waktu telah diedit: 06 Februari 2025, 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEMRContainersServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "eks:DescribeCluster",
        "eks:ListNodeGroups",
        "eks:DescribeNodeGroup",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "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"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonEMRFullAccessPolicy_v2

Deskripsi: Menyediakan akses penuh ke Amazon EMR

`AmazonEMRFullAccessPolicy_v2`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEMRFullAccessPolicy_v2` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 12 Maret 2021, 01:50 UTC
- Waktu yang telah diedit: 27 Maret 2025, 22:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEMRFullAccessPolicy_v2`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RunJobFlowExplicitlyWithEMRManagedTag",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:RunJobFlow"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "ElasticMapReduceActions",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:AddInstanceFleet",
        "elasticmapreduce:AddInstanceGroups",
        "elasticmapreduce:AddJobFlowSteps",
        "elasticmapreduce:AddTags",
        "elasticmapreduce:CancelSteps",
        "elasticmapreduce:CreateEditor",
        "elasticmapreduce: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" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonEMRReadOnlyAccessPolicy_v2

Deskripsi: Menyediakan akses baca saja ke Amazon EMR dan Metrik terkait CloudWatch .

`AmazonEMRReadOnlyAccessPolicy_v2`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEMRReadOnlyAccessPolicy_v2` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 12 Maret 2021, 01:39 UTC
- Waktu telah diedit: Agustus 02, 2023, 19:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEMRReadOnlyAccessPolicy_v2`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ElasticMapReduceActions",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:DescribeEditor",
        "elasticmapreduce:DescribeJobFlows",
        "elasticmapreduce:DescribeSecurityConfiguration",
        "elasticmapreduce:DescribeStep",
        "elasticmapreduce:DescribeReleaseLabel",
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:GetManagedScalingPolicy",
        "elasticmapreduce:GetAutoTerminationPolicy",
        "elasticmapreduce:ListBootstrapActions",
```

```
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListEditors",
        "elasticmapreduce:ListInstanceFleets",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListSecurityConfigurations",
        "elasticmapreduce:ListSteps",
        "elasticmapreduce:ListSupportedInstanceTypes",
        "elasticmapreduce:ViewEventsFromAllClustersInConsole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ViewMetricsInEMRConsole",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonEMRServerlessServiceRolePolicy

Deskripsi: Memungkinkan akses ke sumber daya AWS layanan lain yang diperlukan untuk menjalankan Amazon EMRServerless

`AmazonEMRServerlessServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 20 Mei 2022, 23:15 UTC
- Waktu telah diedit: 25 Januari 2024, 18:21 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEMRServerlessServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2PolicyStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeRouteTables"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchPolicyStatement",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/EMRServerless",
            "AWS/Usage"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonEMRServicePolicy_v2

Deskripsi: Kebijakan ini digunakan untuk Peran Layanan EMR Amazon dan TIDAK boleh digunakan untuk pengguna atau peran IAM lainnya di akun Anda. Kebijakan ini memberikan izin untuk membuat dan mengelola sumber daya yang terkait dengan EMR dan layanan terkait yang diperlukan untuk pengoperasian klaster EMR Anda.

`AmazonEMRServicePolicy_v2`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEMRServicePolicy_v2` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 12 Maret 2021, 01:11 UTC
- Waktu telah diedit: 03 Maret 2025, 20:37 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEMRServicePolicy_v2`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateInTaggedNetwork",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:RunInstances",
        "ec2:CreateFleet",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
```

```
    {
      "Sid" : "CreateWithEMRTaggedLaunchTemplate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateFleet",
        "ec2:RunInstances",
        "ec2:CreateLaunchTemplateVersion"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "CreateEMRTaggedLaunchTemplate",
      "Effect" : "Allow",
      "Action" : "ec2:CreateLaunchTemplate",
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "CreateEMRTaggedInstancesAndVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateFleet"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
```

```
      "Sid" : "ResourcesToLaunchEC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateFleet",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*::image/ami-*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:capacity-reservation/*",
        "arn:aws:ec2:*:*:placement-group/EMR_*",
        "arn:aws:ec2:*:*:fleet/*",
        "arn:aws:ec2:*:*:dedicated-host/*",
        "arn:aws:resource-groups:*:*:group/*"
      ]
    },
    {
      "Sid" : "ManageEMRTaggedResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyInstanceAttribute",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "ManageTagsOnEMRTaggedResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "CreateNetworkInterfaceNeededForPrivateSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "TagOnCreateTaggedEMRResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances",
            "CreateFleet",
            "CreateLaunchTemplate",
```

```
            "CreateNetworkInterface"
          ]
        }
      }
    },
    {
      "Sid" : "TagPlacementGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:placement-group/EMR_*"
      ]
    },
    {
      "Sid" : "ListActionsForEC2Resources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2: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"
        }
      }
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonESCognitoAccess

Deskripsi: Menyediakan akses terbatas ke layanan konfigurasi Amazon Cognito.

`AmazonESCognitoAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonESCognitoAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 Februari 2018, 22:29 UTC
- Waktu yang telah diedit: 20 Desember 2021 14:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonESCognitoAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:DescribeUserPool",
        "cognito-idp:CreateUserPoolClient",
        "cognito-idp:DeleteUserPoolClient",
        "cognito-idp:UpdateUserPoolClient",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:AdminInitiateAuth",
        "cognito-idp:AdminUserGlobalSignOut",
        "cognito-idp:ListUserPoolClients",
        "cognito-identity:DescribeIdentityPool",
        "cognito-identity:UpdateIdentityPool",
        "cognito-identity:SetIdentityPoolRoles",
        "cognito-identity:GetIdentityPoolRoles"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "cognito-identity.amazonaws.com",
            "cognito-identity-us-gov.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonESFullAccess

Deskripsi: Menyediakan akses penuh ke layanan konfigurasi Amazon ES.

`AmazonESFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonESFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Oktober 2015, 19:14 UTC
- Waktu telah diedit: 01 Oktober 2015, 19:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonESFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonESReadOnlyAccess

Deskripsi: Menyediakan akses hanya-baca ke layanan konfigurasi Amazon ES.

`AmazonESReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonESReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Oktober 2015, 19:18 UTC
- Waktu telah diedit: 03 Oktober 2018, 03:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonESReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonEventBridgeApiDestinationsServiceRolePolicy

Deskripsi: Memungkinkan EventBridge untuk mengakses sumber daya Secret Manager atas nama Anda.

`AmazonEventBridgeApiDestinationsServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 11 Februari 2021, 20:52 UTC
- Waktu yang telah diedit: 29 Mei 2025, 21:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEventBridgeApiDestinationsServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:events!connection/*",
      "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"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonEventBridgeFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon EventBridge.

`AmazonEventBridgeFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEventBridgeFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 11 Juli 2019, 14:08 UTC

- Waktu telah diedit: 22 Januari 2025, 01:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeFullAccess`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EventBridgeActions",
      "Effect" : "Allow",
      "Action" : [
        "events:*",
        "schemas:*",
        "scheduler:*",
        "pipes:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMCreateServiceLinkedRoleForApiDestinations",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
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"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonEventBridgePipesFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon EventBridge Pipes.

`AmazonEventBridgePipesFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEventBridgePipesFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Desember 2022, 17:03 UTC
- Waktu yang telah diedit: 01 Desember 2022, 17.03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgePipesFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EventBridgePipesActions",
      "Effect" : "Allow",
      "Action" : "pipes:*",
      "Resource" : "*"
    },
    {
      "Sid" : "IAMPassRoleAccessForPipes",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "pipes.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonEventBridgePipesOperatorAccess

Deskripsi: Menyediakan akses read-only dan operator (kemampuan untuk Menghentikan dan Mulai menjalankan Pipa) ke Amazon EventBridge Pipes.

`AmazonEventBridgePipesOperatorAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEventBridgePipesOperatorAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Desember 2022, 17:04 UTC
- Waktu yang telah diedit: 01 Desember 2022, 17.04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgePipesOperatorAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "pipes:DescribePipe",
        "pipes:ListPipes",
        "pipes:ListTagsForResource",
        "pipes:StartPipe",
        "pipes:StopPipe"
```

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonEventBridgePipesReadOnlyAccess

Deskripsi: Menyediakan akses hanya-baca ke Amazon EventBridge Pipes.

`AmazonEventBridgePipesReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEventBridgePipesReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Desember 2022, 17:04 UTC
- Waktu yang telah diedit: 01 Desember 2022, 17.04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgePipesReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonEventBridgeReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon EventBridge.

`AmazonEventBridgeReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEventBridgeReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 11 Juli 2019, 13:59 UTC
- Waktu yang telah diedit: 01 Desember 2022, 17.02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:DescribeEventBus",
        "events:DescribeEventSource",
        "events:ListEventBuses",
        "events:ListEventSources",
        "events:ListRuleNamesByTarget",
        "events:ListRules",
        "events:ListTargetsByRule",
        "events:TestEventPattern",
        "events:DescribeArchive",
        "events:ListArchives",
        "events:DescribeReplay",
        "events:ListReplays",
        "events:DescribeConnection",
        "events:ListConnections",
        "events:DescribeApiDestination",
        "events:ListApiDestinations",
        "events:DescribeEndpoint",
        "events:ListEndpoints",
        "schemas:DescribeCodeBinding",
        "schemas:DescribeDiscoverer",
```

```
        "schemas:DescribeRegistry",
        "schemas:DescribeSchema",
        "schemas:ExportSchema",
        "schemas:GetCodeBindingSource",
        "schemas:GetDiscoveredSchema",
        "schemas:GetResourcePolicy",
        "schemas:ListDiscoverers",
        "schemas:ListRegistries",
        "schemas:ListSchemas",
        "schemas:ListSchemaVersions",
        "schemas:ListTagsForResource",
        "schemas:SearchSchemas",
        "scheduler:GetSchedule",
        "scheduler:GetScheduleGroup",
        "scheduler:ListSchedules",
        "scheduler:ListScheduleGroups",
        "scheduler:ListTagsForResource",
        "pipes:DescribePipe",
        "pipes:ListPipes",
        "pipes:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonEventBridgeSchedulerFullAccess

Deskripsi: Kebijakan AmazonEventBridgeSchedulerFullAccess terkelola memberikan izin untuk menggunakan semua tindakan EventBridge Penjadwal untuk jadwal, dan grup jadwal.

`AmazonEventBridgeSchedulerFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEventBridgeSchedulerFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 10 November 2022, 18:37 UTC
- Waktu yang telah diedit: 16 Mei 2025, 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeSchedulerFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "scheduler:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "scheduler.amazonaws.com"
        }
      }
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonEventBridgeSchedulerReadOnlyAccess

Deskripsi: Kebijakan AmazonEventBridgeSchedulerReadOnlyAccess terkelola memberikan izin hanya-baca untuk melihat detail tentang jadwal dan grup jadwal

`AmazonEventBridgeSchedulerReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEventBridgeSchedulerReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 10 November 2022, 18:50 UTC
- Waktu yang telah diedit: 16 Mei 2025, 16:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeSchedulerReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "scheduler:ListSchedules",
        "scheduler:ListScheduleGroups",
        "scheduler:GetSchedule",
        "scheduler:GetScheduleGroup",
        "scheduler:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonEventBridgeSchemasFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon EventBridge Schemas.

`AmazonEventBridgeSchemasFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEventBridgeSchemasFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 November 2019, 23:12 UTC
- Waktu yang telah diedit: 28 November 2019, 23:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeSchemasFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonEventBridgeSchemasFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "schemas:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonEventBridgeManageRule",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:EnableRule",
        "events:DisableRule",
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:ListTargetsByRule"
      ],
```

```
      "Resource" : "arn:aws:events:*:*:rule/*Schemas*"
    },
    {
      "Sid" : "IAMCreateServiceLinkedRoleForAmazonEventBridgeSchemas",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/schemas.amazonaws.com/
AWSServiceRoleForSchemas"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonEventBridgeSchemasReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon EventBridge Schemas.

`AmazonEventBridgeSchemasReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEventBridgeSchemasReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 November 2019, 23:05 UTC
- Waktu yang telah diedit: 01 Mei 2020, 00:50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeSchemasReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonEventBridgeSchemasReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "schemas:ListDiscoverers",
        "schemas:DescribeDiscoverer",
        "schemas:ListRegistries",
        "schemas:DescribeRegistry",
        "schemas:SearchSchemas",
        "schemas:ListSchemas",
        "schemas:ListSchemaVersions",
        "schemas:DescribeSchema",
        "schemas:GetDiscoveredSchema",
        "schemas:DescribeCodeBinding",
        "schemas:GetCodeBindingSource",
        "schemas:ListTagsForResource",
        "schemas:GetResourcePolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonEventBridgeSchemasServiceRolePolicy

Deskripsi: Memberikan izin untuk Aturan Terkelola yang dibuat oleh skema Amazon EventBridge .

`AmazonEventBridgeSchemasServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 27 November 2019, 01:10 UTC
- Waktu yang telah diedit: 27 November 2019, 01:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEventBridgeSchemasServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:EnableRule",
        "events:DisableRule",
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:ListTargetsByRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/*Schemas-*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonEVSServiceRolePolicy

Deskripsi: Memberikan izin kepada EVS untuk mengelola sumber daya atas nama Anda

`AmazonEVSServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 16 Mei 2025, 23:37 UTC
- Waktu yang telah diedit: 16 Mei 2025, 23:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEVSServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeNetworkStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateEniInSubnetStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "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" : "UpdateSecurityGroupStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
```

```
      "Resource" : "arn:aws:ec2:*:*:security-group/*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonFISServiceRolePolicy

Deskripsi: Kebijakan untuk memungkinkan AWS FIS mengelola pemantauan dan pemilihan sumber daya untuk eksperimen.

`AmazonFISServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 21 Desember 2020 21:18 UTC
- Waktu yang telah diedit: 25 Oktober 2022 09.05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonFISServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EventBridge",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:DeleteRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "fis.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EventBridgeDescribe",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Tagging",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmHistory"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeUserResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeSubnets",
        "iam:GetUser",
        "iam:GetRole",
        "iam:ListUsers",
        "iam:ListRoles",
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstances",
        "ecs:DescribeClusters",
        "ecs:DescribeTasks",
        "ecs:ListTasks",
        "eks:DescribeNodegroup",
        "eks:DescribeCluster"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonForecastFullAccess

Deskripsi: Memberikan akses ke semua tindakan untuk Amazon Forecast

`AmazonForecastFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonForecastFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 Januari 2019, 01:52 UTC
- Waktu yang telah diedit: 18 Januari 2019, 01:52 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonForecastFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "forecast:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "forecast.amazonaws.com"
        }
      }
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonFraudDetectorFullAccessPolicy

Deskripsi: Memberikan akses ke semua tindakan untuk Amazon Fraud Detector

`AmazonFraudDetectorFullAccessPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonFraudDetectorFullAccessPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 Desember 2019 22:46 UTC
- Waktu yang telah diedit: 03 Desember 2019, 22:46 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFraudDetectorFullAccessPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "frauddetector:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListEndpoints",
        "sagemaker:DescribeEndpoint"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "iam:PassedToService" : "frauddetector.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonFreeRTOSFullAccess

Deskripsi: Kebijakan Akses Penuh untuk Amazon FreeRTOS

`AmazonFreeRTOSFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonFreeRTOSFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 November 2017, 15:32 UTC
- Waktu telah diedit: 29 November 2017, 15:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFreeRTOSFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonFreeRTOSOTAUpdate

Deskripsi: Memungkinkan pengguna untuk mengakses Amazon FreeRTOS OTA Update

`AmazonFreeRTOSOTAUpdate`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonFreeRTOSOTAUpdate` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 27 Agustus 2018, 22:43 UTC
- Waktu yang telah diedit: 18 Desember 2020, 17:47 UTC

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

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonFSxConsoleFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon FSx dan akses ke AWS layanan terkait melalui AWS Management Console.

`AmazonFSxConsoleFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonFSxConsoleFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 November 2018, 16:36 UTC
- Waktu yang telah diedit: 25 Juni 2025, 17:52 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFSxConsoleFullAccess`

Versi kebijakan

Versi kebijakan: v13 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonFSxConsoleReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon FSx dan akses ke AWS layanan terkait melalui AWS Management Console.

`AmazonFSxConsoleReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonFSxConsoleReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 November 2018, 16:35 UTC
- Waktu yang telah diedit: 25 Februari 2025, 15:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFSxConsoleReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonFSxFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon FSx dan akses ke AWS layanan terkait.

`AmazonFSxFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonFSxFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 November 2018, 16:34 UTC
- Waktu yang telah diedit: 25 Juni 2025, 17:52 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFSxFullAccess`

Versi kebijakan

Versi kebijakan: v11 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonFSxReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon FSx.

`AmazonFSxReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonFSxReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 November 2018, 16:33 UTC
- Waktu telah diedit: 28 November 2018, 16:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFSxReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonFSxServiceRolePolicy

Deskripsi: Memungkinkan Amazon FSx mengelola AWS sumber daya atas nama Anda

`AmazonFSxServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 28 November 2018, 10:38 UTC
- Waktu yang telah diedit: 10 Januari 2024, 20:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonFSxServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateFileSystem",
      "Effect" : "Allow",
      "Action" : [
        "ds:AuthorizeApplication",
        "ds:GetAuthorizedApplicationDetails",
        "ds:UnauthorizeApplication",
        "ec2:CreateNetworkInterface",
```

```
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeAddresses",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DisassociateAddress",
        "ec2:GetSecurityGroupsForVpc",
        "route53:AssociateVPCWithHostedZone"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PutMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/FSx"
        }
      }
    },
    {
      "Sid" : "TagResourceNetworkInterface",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        },
        "ForAllValues:StringEquals" : {
```

```
          "aws:TagKeys" : "AmazonFSx.FileSystemId"
        }
      }
    },
    {
      "Sid" : "ManageNetworkInterface",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignPrivateIpAddresses",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonFSx.FileSystemId" : "false"
        }
      }
    },
    {
      "Sid" : "ManageRouteTable",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateRoute",
        "ec2:ReplaceRoute",
        "ec2:DeleteRoute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:route-table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonFSx" : "ManagedByAmazonFSx"
        }
      }
    },
    {
      "Sid" : "PutCloudWatchLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
```

```
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/fsx/*"
    },
    {
      "Sid" : "ManageAuditLogs",
      "Effect" : "Allow",
      "Action" : [
        "firehose:DescribeDeliveryStream",
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : "arn:aws:firehose:*:*:deliverystream/aws-fsx-*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonGlacierFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Glacier melalui. AWS Management Console

`AmazonGlacierFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonGlacierFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu telah diedit: 06 Februari 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGlacierFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonGlacierReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon Glacier melalui. AWS Management Console

`AmazonGlacierReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonGlacierReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu telah diedit: 05 Mei 2016, 18:46 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGlacierReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "glacier:DescribeJob",
        "glacier:DescribeVault",
        "glacier:GetDataRetrievalPolicy",
        "glacier:GetJobOutput",
        "glacier:GetVaultAccessPolicy",
        "glacier:GetVaultLock",
        "glacier:GetVaultNotifications",
        "glacier:ListJobs",
        "glacier:ListMultipartUploads",
        "glacier:ListParts",
        "glacier:ListTagsForVault",
        "glacier:ListVaults"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonGrafanaAthenaAccess

Deskripsi: Kebijakan ini memberikan akses ke Amazon Athena dan dependensi yang diperlukan untuk mengaktifkan kueri dan penulisan hasil ke s3 dari plugin Amazon Athena di Amazon Grafana.

`AmazonGrafanaAthenaAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonGrafanaAthenaAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 22 November 2021 17:11 UTC
- Waktu yang telah diedit: 22 November 2021, 17:11 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonGrafanaAthenaAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetTableMetadata",
        "athena:ListDatabases",
        "athena:ListDataCatalogs",
        "athena:ListTableMetadata",
        "athena:ListWorkGroups"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetWorkGroup",
        "athena:StartQueryExecution",
        "athena:StopQueryExecution"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/GrafanaDataSource" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:BatchGetPartition"
```

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonGrafanaCloudWatchAccess

Deskripsi: Kebijakan ini memberikan akses ke Amazon CloudWatch dan dependensi yang diperlukan untuk digunakan CloudWatch sebagai sumber data dalam Grafana Terkelola Amazon.

`AmazonGrafanaCloudWatchAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonGrafanaCloudWatchAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 24 Maret 2023, 22:41 UTC
- Waktu telah diedit: 24 Maret 2023, 22:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonGrafanaCloudWatchAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetInsightRuleReport"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups",
        "logs:GetLogGroupFields",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:GetQueryResults",
        "logs:GetLogEvents"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeTags",
        "ec2:DescribeInstances",
        "ec2:DescribeRegions"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "tag:GetResources",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:ListSinks",
        "oam:ListAttachedLinks"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonGrafanaRedshiftAccess

Deskripsi: Kebijakan ini memberikan akses terbatas ke Amazon Redshift dan dependensi yang diperlukan untuk menggunakan plugin Amazon Redshift di Amazon Grafana.

`AmazonGrafanaRedshiftAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonGrafanaRedshiftAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 26 November 2021 23:15 UTC
- Waktu yang telah diedit: 26 November 2021, 23:15 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonGrafanaRedshiftAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters",
        "redshift-data:GetStatementResult",
        "redshift-data:DescribeStatement",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:DescribeTable",
        "redshift-data:ExecuteStatement",
        "redshift-data:ListTables",
        "redshift-data:ListSchemas"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/GrafanaDataSource" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "redshift:GetClusterCredentials",
      "Resource" : [
        "arn:aws:redshift:*:*:dbname:*/*",
        "arn:aws:redshift:*:*:dbuser:*/redshift_data_api_user"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "secretsmanager:ResourceTag/RedshiftQueryOwner" : "false"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonGrafanaServiceLinkedRolePolicy

Deskripsi: Menyediakan akses ke AWS Sumber Daya yang dikelola atau digunakan oleh Amazon Grafana.

`AmazonGrafanaServiceLinkedRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 08 November 2022, 23:10 UTC
- Waktu telah diedit: 08 November 2022, 23.10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonGrafanaServiceLinkedRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonGrafanaManaged"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        },
        "Null" : {
          "aws:RequestTag/AmazonGrafanaManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:DeleteNetworkInterface",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AmazonGrafanaManaged" : "false"
        }
      }
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonGuardDutyFullAccess

Deskripsi: Menyediakan akses penuh untuk menggunakan Amazon GuardDuty.

`AmazonGuardDutyFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonGuardDutyFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 November 2017, 22:31 UTC
- Waktu yang telah diedit: 10 Juni 2024, 22:50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGuardDutyFullAccess`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
  "Statement" : [
    {
      "Sid" : "AmazonGuardDutyFullAccessSid1",
      "Effect" : "Allow",
      "Action" : "guardduty:*",
      "Resource" : "*"
    },
    {
      "Sid" : "CreateServiceLinkedRoleSid1",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : [
            "guardduty.amazonaws.com",
            "malware-protection.guardduty.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ActionsForOrganizationsSid1",
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IamGetRoleSid1",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/
*AWSServiceRoleForAmazonGuardDutyMalwareProtection"
    },
    {
```

```
      "Sid" : "AllowPassRoleToMalwareProtectionPlan",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "malware-protection-plan.guardduty.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonGuardDutyFullAccess_v2

Deskripsi: Menyediakan akses penuh untuk menggunakan Amazon GuardDuty

`AmazonGuardDutyFullAccess_v2`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonGuardDutyFullAccess_v2` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 04 Juni 2025, 20:22 UTC
- Waktu yang telah diedit: 04 Juni 2025, 20:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGuardDutyFullAccess_v2`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "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" : "PassRoleToMalwareProtectionPlan",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "malware-protection-plan.guardduty.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonGuardDutyMalwareProtectionServiceRolePolicy

Deskripsi: perlindungan GuardDuty malware menggunakan peran terkait layanan (SLR) bernama. AWSService RoleForAmazonGuardDutyMalwareProtection Peran terkait layanan ini memungkinkan perlindungan GuardDuty malware melakukan pemindaian tanpa agen untuk mendeteksi malware. Ini memungkinkan GuardDuty untuk membuat snapshot di akun Anda, dan berbagi snapshot dengan akun GuardDuty layanan untuk memindai malware. Ini mengevaluasi snapshot bersama ini dan menyertakan metadata EC2 instance yang diambil dalam temuan Perlindungan Malware. GuardDuty Peran AWSService RoleForAmazonGuardDutyMalwareProtection terkait layanan mempercayai layanan malware-protection.guardduty.amazonaws.com untuk mengambil peran tersebut.

`AmazonGuardDutyMalwareProtectionServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 19 Juli 2022, 19:06 UTC
- Waktu telah diedit: 25 Januari 2024, 22:24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonGuardDutyMalwareProtectionServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeAndListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots",
        "ecs:ListClusters",
        "ecs:ListContainerInstances",
        "ecs:ListTasks",
        "ecs:DescribeTasks",
        "eks:DescribeCluster"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateSnapshotVolumeConditionalStatement",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshot",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/GuardDutyExcluded" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotConditionalStatement",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshot",
```

```
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "GuardDutyScanId"
        }
      }
    },
    {
      "Sid" : "CreateTagsPermission",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:*/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateSnapshot"
        }
      }
    },
    {
      "Sid" : "AddTagsToSnapshotPermission",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/GuardDutyScanId" : "*"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "GuardDutyExcluded",
            "GuardDutyFindingDetected"
          ]
        }
      }
    },
    {
      "Sid" : "DeleteAndShareSnapshotPermission",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot",
        "ec2:ModifySnapshotAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
```

```
        "StringLike" : {
          "ec2:ResourceTag/GuardDutyScanId" : "*"
        },
        "Null" : {
          "aws:ResourceTag/GuardDutyExcluded" : "true"
        }
      }
    },
    {
      "Sid" : "PreventPublicAccessToSnapshotPermission",
      "Effect" : "Deny",
      "Action" : [
        "ec2:ModifySnapshotAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:Add/group" : "all"
        }
      }
    },
    {
      "Sid" : "CreateGrantPermission",
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/GuardDutyExcluded" : "true"
        },
        "StringLike" : {
          "kms:EncryptionContext:aws:ebs:id" : "snap-*"
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt",
            "CreateGrant",
            "GenerateDataKeyWithoutPlaintext",
            "ReEncryptFrom",
            "ReEncryptTo",
            "RetireGrant",
            "DescribeKey"
          ]
        },
```

```
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        }
      }
    },
    {
      "Sid" : "ShareSnapshotKMSPermission",
      "Effect" : "Allow",
      "Action" : [
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com"
        },
        "Null" : {
          "aws:ResourceTag/GuardDutyExcluded" : "true"
        }
      }
    },
    {
      "Sid" : "DescribeKeyPermission",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
      "Sid" : "GuardDutyLogGroupPermission",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups",
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/guardduty/*"
    },
    {
      "Sid" : "GuardDutyLogStreamPermission",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
```

```
        "logs:DescribeLogStreams"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/guardduty/*:log-stream:*"
    },
    {
      "Sid" : "EBSDirectAPIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ebs:GetSnapshotBlock",
        "ebs:ListSnapshotBlocks"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/GuardDutyScanId" : "*"
        },
        "Null" : {
          "aws:ResourceTag/GuardDutyExcluded" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonGuardDutyReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke GuardDuty sumber daya Amazon

`AmazonGuardDutyReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonGuardDutyReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 November 2017, 22:29 UTC
- Waktu telah diedit: 16 November 2023, 23:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGuardDutyReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "guardduty:Describe*",
        "guardduty:Get*",
        "guardduty:List*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonGuardDutyServiceRolePolicy

Deskripsi: Aktifkan akses ke AWS Sumber Daya yang digunakan atau dikelola oleh Amazon Guard Duty

`AmazonGuardDutyServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 28 November 2017, 20:12 UTC
- Waktu yang telah diedit: Agustus 12, 2024, 20:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonGuardDutyServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v10 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GuardDutyGetDescribeListPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeImages",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeTransitGatewayAttachments",
        "organizations:ListAccounts",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetEncryptionConfiguration",
        "s3:GetBucketTagging",
        "s3:GetAccountPublicAccessBlock",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "lambda:GetFunctionConfiguration",
        "lambda:ListTags",
        "eks:ListClusters",
        "eks:DescribeCluster",
        "ec2:DescribeVpcEndpointServices",
        "ec2: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" : "*"
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonHealthLakeFullAccess

Deskripsi: Menyediakan akses penuh ke HealthLake layanan Amazon.

`AmazonHealthLakeFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonHealthLakeFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 17 Februari 2021, 01:07 UTC
- Waktu yang telah diedit: 17 Februari 2021, 01:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHealthLakeFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "healthlake:*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "iam:ListRoles"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "healthlake.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonHealthLakeReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke HealthLake layanan Amazon.

`AmazonHealthLakeReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonHealthLakeReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 17 Februari 2021 02:43 UTC
- Waktu yang telah diedit: 17 Februari 2021 02:43 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHealthLakeReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "healthlake:ListFHIRDatastores",
        "healthlake:DescribeFHIRDatastore",
        "healthlake:DescribeFHIRImportJob",
        "healthlake:DescribeFHIRExportJob",
        "healthlake:GetCapabilities",
        "healthlake:ReadResource",
        "healthlake:SearchWithGet",
        "healthlake:SearchWithPost"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonHoneycodeFullAccess

Deskripsi: Menyediakan akses penuh ke Honeycode melalui AWS Management Console dan SDK.

`AmazonHoneycodeFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonHoneycodeFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 24 Juni 2020, 20:28 UTC
- Waktu yang telah diedit: 24 Juni 2020, 20:28 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonHoneycodeReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Honeycode melalui AWS Management Console dan SDK.

`AmazonHoneycodeReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonHoneycodeReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 24 Juni 2020, 20:28 UTC
- Waktu yang telah diedit: 01 Desember 2020, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonHoneycodeServiceRolePolicy

Deskripsi: Peran terkait layanan yang diperlukan Amazon Honeycode untuk mengakses sumber daya Anda.

`AmazonHoneycodeServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 18 November 2020, 18:03 UTC
- Waktu yang telah diedit: 18 November 2020, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonHoneycodeServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonHoneycodeTeamAssociationFullAccess

Deskripsi: Menyediakan akses penuh ke Honeycode Team Association melalui AWS Management Console dan SDK.

`AmazonHoneycodeTeamAssociationFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonHoneycodeTeamAssociationFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 24 Juni 2020, 20:28 UTC
- Waktu yang telah diedit: 24 Juni 2020, 20:28 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeTeamAssociationFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
  "Statement" : [
    {
      "Action" : [
        "honeycode:ListTeamAssociations",
        "honeycode:ApproveTeamAssociation",
        "honeycode:RejectTeamAssociation"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonHoneycodeTeamAssociationReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Honeycode Team Association melalui AWS Management Console dan SDK.

`AmazonHoneycodeTeamAssociationReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonHoneycodeTeamAssociationReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 24 Juni 2020, 20:27 UTC
- Waktu yang telah diedit: 24 Juni 2020, 20:27 UTC

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

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonHoneycodeWorkbookFullAccess

Deskripsi: Menyediakan akses penuh ke Honeycode Workbook melalui AWS Management Console dan SDK.

`AmazonHoneycodeWorkbookFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonHoneycodeWorkbookFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 24 Juni 2020, 20:28 UTC
- Waktu yang telah diedit: 01 Desember 2020, 17:30 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeWorkbookFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "honeycode:GetScreenData",
        "honeycode:InvokeScreenAutomation",
        "honeycode:BatchCreateTableRows",
        "honeycode:BatchDeleteTableRows",
        "honeycode:BatchUpdateTableRows",
        "honeycode:BatchUpsertTableRows",
        "honeycode:DescribeTableDataImportJob",
        "honeycode:ListTableColumns",
        "honeycode:ListTableRows",
        "honeycode:ListTables",
        "honeycode:QueryTableRows",
        "honeycode:StartTableDataImportJob"
```

```
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonHoneycodeWorkbookReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Buku Kerja Honeycode melalui AWS Management Console dan SDK.

`AmazonHoneycodeWorkbookReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonHoneycodeWorkbookReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 24 Juni 2020, 20:28 UTC
- Waktu yang telah diedit: 01 Desember 2020, 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeWorkbookReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "honeycode:GetScreenData",
        "honeycode:DescribeTableDataImportJob",
        "honeycode:ListTableColumns",
        "honeycode:ListTableRows",
        "honeycode:ListTables",
        "honeycode:QueryTableRows"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonInspector2AgentlessServiceRolePolicy

Deskripsi: Memberikan Amazon Inspector akses ke yang diperlukan Layanan AWS untuk melakukan penilaian keamanan tanpa agen

`AmazonInspector2AgentlessServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 20 November 2023, 15:18 UTC
- Waktu telah diedit: 20 November 2023, 15:18 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspector2AgentlessServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "InstanceIdentification",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetSnapshotData",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ebs:ListSnapshotBlocks",
        "ebs:GetSnapshotBlock"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/InspectorScan" : "*"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotsAnyInstanceOrVolume",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshots",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "Sid" : "DenyCreateSnapshotsOnExcludedInstances",
      "Effect" : "Deny",
      "Action" : "ec2:CreateSnapshots",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/InspectorEc2Exclusion" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotsOnAnySnapshotOnlyWithTag",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshots",
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "InspectorScan"
        }
      }
```

```
    },
    {
      "Sid" : "CreateOnlyInspectorScanTagOnlyUsingCreateSnapshots",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "ec2:CreateAction" : "CreateSnapshots"
        },
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "InspectorScan"
        }
      }
    },
    {
      "Sid" : "DeleteOnlySnapshotsTaggedForScanning",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteSnapshot",
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/InspectorScan" : "*"
        }
      }
    },
    {
      "Sid" : "DenyKmsDecryptForExcludedKeys",
      "Effect" : "Deny",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/InspectorEc2Exclusion" : "true"
        }
      }
    },
    {
      "Sid" : "DecryptSnapshotBlocksVolContext",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
```

```
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com",
          "kms:EncryptionContext:aws:ebs:id" : "vol-*"
        }
      }
    },
    {
      "Sid" : "DecryptSnapshotBlocksSnapContext",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com",
          "kms:EncryptionContext:aws:ebs:id" : "snap-*"
        }
      }
    },
    {
      "Sid" : "DescribeKeysForEbsOperations",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ListKeyResourceTags",
      "Effect" : "Allow",
      "Action" : "kms:ListResourceTags",
```

```
      "Resource" : "arn:aws:kms:*:*:key/*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonInspector2FullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Inspector dan akses ke layanan terkait lainnya seperti organisasi.

`AmazonInspector2FullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonInspector2FullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 November 2021 19:10 UTC
- Waktu yang telah diedit: 25 April 2024, 13:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspector2FullAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonInspector2FullAccess_v2

Deskripsi: Menyediakan akses penuh ke Amazon Inspector dan akses ke layanan terkait lainnya seperti organisasi dengan akses organisasi yang terbatas.

`AmazonInspector2FullAccess_v2`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonInspector2FullAccess_v2` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 Juli 2025, 16:07 UTC
- Waktu yang telah diedit: 03 Juli 2025, 16:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspector2FullAccess_v2`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "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:*:organizations::*:ou/o-*/ou-*"
    },
    {
      "Sid" : "AllowAccountsBasedAccessToOrganizationApis",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount"
      ],
      "Resource" : "arn:*:organizations::*:account/o-*/*"
    },
    {
      "Sid" : "AllowAccessToOrganizationApis",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonInspector2ManagedCisPolicy

Deskripsi: Ini adalah kebijakan terkelola yang harus dilampirkan pelanggan pada peran mereka untuk berkomunikasi dengan layanan inspektur untuk pemindaian CIS

`AmazonInspector2ManagedCisPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonInspector2ManagedCisPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 24 Januari 2024, 16:31 UTC
- Waktu telah diedit: 24 Januari 2024, 16:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspector2ManagedCisPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PermissionsForCISScans",
      "Effect" : "Allow",
      "Action" : [
        "inspector2:StartCisSession",
        "inspector2:StopCisSession",
        "inspector2:SendCisSessionTelemetry",
        "inspector2:SendCisSessionHealth"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonInspector2ReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke layanan Amazon inspector2 dan layanan dukungan yang relevan

`AmazonInspector2ReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonInspector2ReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 21 Januari 2022, 14:45 UTC

- Waktu yang telah diedit: September 22, 2023, 20:56 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspector2ReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "inspector2:BatchGet*",
        "inspector2:List*",
        "inspector2:Describe*",
        "inspector2:Get*",
        "inspector2:Search*",
        "codeguru-security:BatchGetFindings",
        "codeguru-security:GetAccountConfiguration"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonInspector2ServiceRolePolicy

Deskripsi: Memberikan Amazon Inspector akses ke yang diperlukan Layanan AWS untuk melakukan penilaian keamanan

`AmazonInspector2ServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 16 November 2021 20:27 UTC
- Waktu telah diedit: 29 April 2025, 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspector2ServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v16 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonInspectorFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Inspector.

`AmazonInspectorFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonInspectorFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 07 Oktober 2015, 17:08 UTC
- Waktu yang telah diedit: 21 Desember 2017, 14:53 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspectorFullAccess`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "inspector:*",
        "ec2:DescribeInstances",
        "ec2:DescribeTags",
        "sns:ListTopics",
        "events:DescribeRule",
        "events:ListRuleNamesByTarget"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "inspector.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/inspector.amazonaws.com/
AWSServiceRoleForAmazonInspector",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "inspector.amazonaws.com"
        }
      }
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonInspectorReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon Inspector.

`AmazonInspectorReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonInspectorReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 07 Oktober 2015, 17:08 UTC
- Waktu yang telah diedit: 01 Oktober 2019, 15:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspectorReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "inspector:Describe*",
        "inspector:Get*",
        "inspector:List*",
        "inspector:Preview*",
        "ec2:DescribeInstances",
        "ec2:DescribeTags",
        "sns:ListTopics",
        "events:DescribeRule",
        "events:ListRuleNamesByTarget"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonInspectorServiceRolePolicy

Deskripsi: Memberikan Amazon Inspector akses ke yang diperlukan Layanan AWS untuk melakukan penilaian keamanan

`AmazonInspectorServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 21 November 2017, 15:48 UTC
- Waktu yang telah diedit: 11 September 2020, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspectorServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonKendraFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Kendra melalui. AWS Management Console

`AmazonKendraFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonKendraFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 Desember 2019, 16:15 UTC
- Waktu yang telah diedit: 03 Desember 2019, 16:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKendraFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "kendra.amazonaws.com"
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DescribeSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonKendra-*"
    },
    {
      "Effect" : "Allow",
      "Action" : "kendra:*",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonKendraReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon Kendra melalui. AWS Management Console

`AmazonKendraReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonKendraReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 03 Desember 2019, 16:13 UTC
- Waktu yang telah diedit: 27 Mei 2021, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKendraReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonKeyspacesFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Keyspaces

`AmazonKeyspacesFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonKeyspacesFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 23 April 2020, 17:06 UTC
- Waktu telah diedit: 30 Juni 2025, 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKeyspacesFullAccess`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeleteScheduledAction",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "application-autoscaling:PutScheduledAction",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget",
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudwatchAlarmsFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ApplicationAutoscalingServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/cassandra.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_CassandraTable",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "cassandra.application-autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "KeyspacesReplicationServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
```

```
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
replication.cassandra.amazonaws.com/AWSServiceRoleForKeyspacesReplication",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "replication.cassandra.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "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" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonKeyspacesReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon Keyspaces

`AmazonKeyspacesReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonKeyspacesReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 23 April 2020, 17:07 UTC
- Waktu yang telah diedit: 30 Juni 2025, 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKeyspacesReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonKeyspacesReadOnlyAccess_v2

Deskripsi: Menyediakan akses baca saja ke Amazon Keyspaces dan layanan terkait AWS .

`AmazonKeyspacesReadOnlyAccess_v2`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonKeyspacesReadOnlyAccess_v2` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 12 September 2023, 17:01 UTC
- Waktu telah diedit: 27 Juni 2025, 22:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKeyspacesReadOnlyAccess_v2`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonKinesisAnalyticsFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Kinesis Analytics melalui AWS Management Console file.

`AmazonKinesisAnalyticsFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonKinesisAnalyticsFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 21 September 2016, 19:01 UTC
- Waktu telah diedit: September 21, 2016, 19:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisAnalyticsFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "kinesisanalytics:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:CreateStream",
        "kinesis:DeleteStream",
        "kinesis:DescribeStream",
        "kinesis:ListStreams",
        "kinesis:PutRecord",
        "kinesis:PutRecords"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:GetLogEvents",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListPolicyVersions",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/service-role/kinesis-analytics*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonKinesisAnalyticsReadOnly

Deskripsi: Menyediakan akses hanya-baca ke Amazon Kinesis Analytics melalui file. AWS Management Console

`AmazonKinesisAnalyticsReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonKinesisAnalyticsReadOnly` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 21 September 2016, 18:16 UTC
- Waktu telah diedit: September 21, 2016, 18:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisAnalyticsReadOnly`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:GetLogEvents",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListPolicyVersions",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonKinesisFirehoseFullAccess

Deskripsi: Menyediakan akses penuh ke semua Aliran Pengiriman Amazon Kinesis Firehose.

`AmazonKinesisFirehoseFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonKinesisFirehoseFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 07 Oktober 2015, 18:45 UTC
- Waktu telah diedit: 07 Oktober 2015, 18:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisFirehoseFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonKinesisFirehoseReadOnlyAccess

Deskripsi: Menyediakan akses hanya baca ke semua Aliran Pengiriman Amazon Kinesis Firehose.

`AmazonKinesisFirehoseReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonKinesisFirehoseReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 07 Oktober 2015, 18:43 UTC
- Waktu telah diedit: 07 Oktober 2015, 18:43 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisFirehoseReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonKinesisFullAccess

Deskripsi: Menyediakan akses penuh ke semua aliran melalui. AWS Management Console

`AmazonKinesisFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonKinesisFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu telah diedit: 06 Februari 2015, 18:40 UTC

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

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonKinesisReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke semua aliran melalui. AWS Management Console

`AmazonKinesisReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonKinesisReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu telah diedit: 06 Februari 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonKinesisVideoStreamsFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Kinesis Video AWS Management Console Streams melalui file.

`AmazonKinesisVideoStreamsFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonKinesisVideoStreamsFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Desember 2017, 23:27 UTC
- Waktu telah diedit: 01 Desember 2017, 23:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisVideoStreamsFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonKinesisVideoStreamsReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke AWS Kinesis Video AWS Management Console Streams melalui file.

`AmazonKinesisVideoStreamsReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonKinesisVideoStreamsReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Desember 2017, 23:14 UTC
- Waktu telah diedit: 01 Desember 2017, 23:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisVideoStreamsReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonLaunchWizard_Fullaccess

Deskripsi: Akses penuh ke Wisaya AWS peluncuran dan layanan lain yang diperlukan.

`AmazonLaunchWizard_Fullaccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonLaunchWizard_Fullaccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Agustus 2020, 17:47 UTC
- Waktu telah diedit: 22 Februari 2023, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLaunchWizard_Fullaccess`

Versi kebijakan

Versi kebijakan: v15 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "applicationinsights:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "resource-groups:List*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:ChangeResourceRecordSets",
        "route53:GetChange",
        "route53:ListResourceRecordSets",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:List*",
        "cloudwatch:Get*",
        "cloudwatch:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateInternetGateway",
        "ec2:CreateNatGateway",
        "ec2:CreateVpc",
        "ec2:CreateKeyPair",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSubnet"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AllocateHosts",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssociateAddress",
        "ec2:CreateDhcpOptions",
        "ec2:CreateEgressOnlyInternetGateway",
        "ec2:CreateNetworkInterface",
        "ec2:CreateVolume",
        "ec2:CreateVpcEndpoint",
        "ec2:CreateTags",
        "ec2:DeleteTags",
```

```
        "ec2:RunInstances",
        "ec2:StartInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVolumeAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:AssociateDhcpOptions",
        "ec2:AssociateSubnetCidrBlock",
        "ec2:AttachInternetGateway",
        "ec2:AttachNetworkInterface",
        "ec2:AttachVolume",
        "ec2:DeleteDhcpOptions",
        "ec2:DeleteInternetGateway",
        "ec2:DeleteKeyPair",
        "ec2:DeleteNatGateway",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteVolume",
        "ec2:DeleteVpc",
        "ec2:DetachInternetGateway",
        "ec2:DetachVolume",
        "ec2:DeleteSnapshot",
        "ec2:AssociateRouteTable",
        "ec2:AssociateVpcCidrBlock",
        "ec2:DeleteNetworkAcl",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
        "ec2:DeleteSubnet",
        "ec2:DetachNetworkInterface",
        "ec2:DisassociateAddress",
        "ec2:DisassociateVpcCidrBlock",
        "ec2:GetLaunchTemplateData",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifyVolume",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:GetConsoleOutput",
        "ec2:GetPasswordData",
        "ec2:ReleaseAddress",
        "ec2:ReplaceRoute",
        "ec2:ReplaceRouteTableAssociation",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DisassociateIamInstanceProfile",
```

```
        "ec2:DisassociateRouteTable",
        "ec2:DisassociateSubnetCidrBlock",
        "ec2:ModifyInstancePlacement",
        "ec2:DeletePlacementGroup",
        "ec2:CreatePlacementGroup",
        "elasticfilesystem:DeleteFileSystem",
        "elasticfilesystem:DeleteMountTarget",
        "ds:AddIpRoutes",
        "ds:CreateComputer",
        "ds:CreateMicrosoftAD",
        "ds:DeleteDirectory",
        "servicecatalog:AssociateProductWithPortfolio",
        "cloudformation:GetTemplateSummary",
        "sts:GetCallerIdentity"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStack*",
        "cloudformation:Get*",
        "cloudformation:ListStacks",
        "cloudformation:SignalResource",
        "cloudformation:DeleteStack"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/LaunchWizard*/*",
        "arn:aws:cloudformation:*:*:stack/ApplicationInsights*/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/LaunchWizard-*/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:AddRoleToInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonEC2RoleForLaunchWizard*",
        "arn:aws:iam::*:instance-profile/LaunchWizard*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonEC2RoleForLaunchWizard*",
        "arn:aws:iam::*:role/service-role/AmazonLambdaRoleForLaunchWizard*",
        "arn:aws:iam::*:instance-profile/LaunchWizard*"
      ],
      "Condition" : {
        "StringEqualsIfExists" : {
          "iam:PassedToService" : [
            "lambda.amazonaws.com",
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:AttachInstances",
        "autoscaling:CreateAutoScalingGroup",
```

```
        "autoscaling:CreateLaunchConfiguration",
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:DeleteLaunchConfiguration",
        "autoscaling:UpdateAutoScalingGroup",
        "autoscaling:CreateOrUpdateTags",
        "logs:CreateLogStream",
        "logs:DeleteLogGroup",
        "logs:DeleteLogStream",
        "logs:DescribeLog*",
        "logs:PutLogEvents",
        "resource-groups:CreateGroup",
        "resource-groups:DeleteGroup",
        "sns:ListSubscriptionsByTopic",
        "sns:Publish",
        "ssm:DeleteDocument",
        "ssm:DeleteParameter*",
        "ssm:DescribeDocument*",
        "ssm:GetDocument",
        "ssm:PutParameter"
      ],
      "Resource" : [
        "arn:aws:resource-groups:*:*:group/LaunchWizard*",
        "arn:aws:sns:*:*:*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/
LaunchWizard*",
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/
LaunchWizard*",
        "arn:aws:ssm:*:*:parameter/LaunchWizard*",
        "arn:aws:ssm:*:*:document/LaunchWizard*",
        "arn:aws:logs:*:*:log-group:*:*:*",
        "arn:aws:logs:*:*:log-group:LaunchWizard*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetDocument",
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ssm:*::document/AWS-RunShellScript"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/LaunchWizard-*/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DeleteLogStream",
        "logs:GetLogEvents",
        "logs:PutLogEvents",
        "ssm:AddTagsToResource",
        "ssm:DescribeDocument",
        "ssm:GetDocument",
        "ssm:ListTagsForResource",
        "ssm:RemoveTagsFromResource"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:*:*:*",
        "arn:aws:logs:*:*:log-group:LaunchWizard*",
        "arn:aws:ssm:*:*:parameter/LaunchWizard*",
        "arn:aws:ssm:*:*:document/LaunchWizard*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:Describe*",
        "cloudformation:DescribeAccountLimits",
        "cloudformation:DescribeStackDriftDetectionStatus",
        "cloudformation:List*",
        "cloudformation:ValidateTemplate",
        "ds:Describe*",
        "ds:ListAuthorizedApplications",
        "ec2:Describe*",
```

```
        "ec2:Get*",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:GetUser",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:List*",
        "logs:CreateLogGroup",
        "logs:GetLogDelivery",
        "logs:GetLogRecord",
        "logs:ListLogDeliveries",
        "resource-groups:Get*",
        "resource-groups:List*",
        "servicequotas:GetServiceQuota",
        "servicequotas:ListServiceQuotas",
        "sns:ListSubscriptions",
        "sns:ListTopics",
        "ssm:CreateDocument",
        "ssm:DescribeAutomation*",
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeParameters",
        "ssm:GetAutomationExecution",
        "ssm:GetCommandInvocation",
        "ssm:GetParameter*",
        "ssm:GetConnectionStatus",
        "ssm:ListCommand*",
        "ssm:ListDocument*",
        "ssm:ListInstanceAssociations",
        "ssm:SendAutomationSignal",
        "tag:Get*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution",
        "ssm:StopAutomationExecution"
      ],
      "Resource" : "arn:aws:ssm:*:*:automation-definition/LaunchWizard-*:*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:GetLog*",
      "Resource" : [
        "arn:aws:logs:*:*:log-group:*:*:*",
        "arn:aws:logs:*:*:log-group:LaunchWizard*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:List*",
        "cloudformation:Describe*"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/LaunchWizard*/"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "autoscaling.amazonaws.com",
            "application-insights.amazonaws.com",
            "events.amazonaws.com",
            "autoscaling.amazonaws.com.cn",
            "events.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "launchwizard:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "sqs:TagQueue",
        "sqs:GetQueueUrl",
        "sqs:AddPermission",
        "sqs:ListQueues",
        "sqs:DeleteQueue",
        "sqs:GetQueueAttributes",
        "sqs:ListQueueTags",
        "sqs:CreateQueue",
        "sqs:SetQueueAttributes"
      ],
      "Resource" : "arn:aws:sqs:*:*:LaunchWizard*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "iam:GetInstanceProfile",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:LaunchWizard*",
        "arn:aws:iam::*:instance-profile/LaunchWizard*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "route53:ListHostedZones",
        "ec2:CreateSecurityGroup",
        "ec2:AuthorizeSecurityGroupIngress",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:CreateFileSystem",
        "elasticfilesystem:CreateMountTarget",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeMountTargetSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
```

```
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::launchwizard*",
        "arn:aws:s3:::launchwizard*/*",
        "arn:aws:s3:::aws-sap-data-provider/config.properties"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudformation:TagResource",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "LaunchWizard*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutBucketVersioning",
        "s3:DeleteBucket",
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:LaunchWizard*",
        "arn:aws:s3:::launchwizard*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:CreateTable",
        "dynamodb:DescribeTable",
        "dynamodb:DeleteTable"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/LaunchWizard*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:TagResource",
        "secretsmanager:UntagResource",
        "secretsmanager:PutResourcePolicy",
        "secretsmanager:DeleteResourcePolicy",
        "secretsmanager:ListSecretVersionIds",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:LaunchWizard*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetRandomPassword",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateOpsMetadata"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:DeleteOpsMetadata",
      "Resource" : "arn:aws:ssm:*:*:opsmetadata/aws/ssm/LaunchWizard*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:DeleteTopic",
        "sns:Subscribe",
        "sns:Unsubscribe"
      ],
      "Resource" : "arn:aws:sns:*:*:LaunchWizard*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "fsx:UntagResource",
        "fsx:TagResource",
        "fsx:DeleteFileSystem",
        "fsx:ListTagsForResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/Name" : "LaunchWizard*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "fsx:CreateFileSystem"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/Name" : [
            "LaunchWizard*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeFileSystems"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:CreatePortfolio",
        "servicecatalog:DescribePortfolio",
        "servicecatalog:CreateConstraint",
        "servicecatalog:CreateProduct",
        "servicecatalog:AssociatePrincipalWithPortfolio",
```

```
        "servicecatalog:CreateProvisioningArtifact",
        "servicecatalog:TagResource",
        "servicecatalog:UntagResource"
      ],
      "Resource" : [
        "arn:aws:servicecatalog:*:*:*/*",
        "arn:aws:catalog:*:*:*/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:DeleteAssociation"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/AWS-ConfigureAWSPackage",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:UntagResource",
        "elasticfilesystem:TagResource"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "logs:TagResource",
        "logs:UntagResource"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:LaunchWizard*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonLaunchWizardFullAccessV2

Deskripsi: Akses penuh ke Wisaya AWS peluncuran dan layanan lain yang diperlukan.

`AmazonLaunchWizardFullAccessV2`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonLaunchWizardFullAccessV2` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 September 2023, 17:14 UTC
- Waktu yang telah diedit: September 01, 2023, 17:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLaunchWizardFullAccessV2`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AppInsightsActions0",
      "Effect" : "Allow",
      "Action" : "applicationinsights:*",
      "Resource" : "*"
    },
    {
      "Sid" : "ResourceGroupActions0",
      "Effect" : "Allow",
      "Action" : "resource-groups:List*",
      "Resource" : "*"
    },
    {
      "Sid" : "Route53Actions0",
      "Effect" : "Allow",
      "Action" : [
        "route53:ChangeResourceRecordSets",
        "route53:GetChange",
        "route53:ListResourceRecordSets",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3Actions0",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
```

```
        "s3:GetBucketLocation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KmsActions0",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchActions0",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:List*",
        "cloudwatch:Get*",
        "cloudwatch:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Ec2Actions0",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateInternetGateway",
        "ec2:CreateNatGateway",
        "ec2:CreateVpc",
        "ec2:CreateKeyPair",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSubnet"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Ec2Actions1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AllocateHosts",
        "ec2:AssignPrivateIpAddresses",
```

```
        "ec2:AssociateAddress",
        "ec2:CreateDhcpOptions",
        "ec2:CreateEgressOnlyInternetGateway",
        "ec2:CreateNetworkInterface",
        "ec2:CreateVolume",
        "ec2:CreateVpcEndpoint",
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVolumeAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:AssociateDhcpOptions",
        "ec2:AssociateSubnetCidrBlock",
        "ec2:AttachInternetGateway",
        "ec2:AttachNetworkInterface",
        "ec2:AttachVolume",
        "ec2:DeleteDhcpOptions",
        "ec2:DeleteInternetGateway",
        "ec2:DeleteKeyPair",
        "ec2:DeleteNatGateway",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteVolume",
        "ec2:DeleteVpc",
        "ec2:DetachInternetGateway",
        "ec2:DetachVolume",
        "ec2:DeleteSnapshot",
        "ec2:AssociateRouteTable",
        "ec2:AssociateVpcCidrBlock",
        "ec2:DeleteNetworkAcl",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
        "ec2:DeleteSubnet",
        "ec2:DetachNetworkInterface",
        "ec2:DisassociateAddress",
        "ec2:DisassociateVpcCidrBlock",
        "ec2:GetLaunchTemplateData",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifyVolume",
        "ec2:AuthorizeSecurityGroupEgress",
```

```
        "ec2:GetConsoleOutput",
        "ec2:GetPasswordData",
        "ec2:ReleaseAddress",
        "ec2:ReplaceRoute",
        "ec2:ReplaceRouteTableAssociation",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DisassociateIamInstanceProfile",
        "ec2:DisassociateRouteTable",
        "ec2:DisassociateSubnetCidrBlock",
        "ec2:ModifyInstancePlacement",
        "ec2:DeletePlacementGroup",
        "ec2:CreatePlacementGroup",
        "elasticfilesystem:DeleteFileSystem",
        "elasticfilesystem:DeleteMountTarget",
        "ds:AddIpRoutes",
        "ds:CreateComputer",
        "ds:CreateMicrosoftAD",
        "ds:DeleteDirectory",
        "servicecatalog:AssociateProductWithPortfolio",
        "cloudformation:GetTemplateSummary",
        "sts:GetCallerIdentity"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudFormationActions0",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStack*",
        "cloudformation:Get*",
        "cloudformation:ListStacks",
        "cloudformation:SignalResource",
        "cloudformation:DeleteStack"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/LaunchWizard*/*",
        "arn:aws:cloudformation:*:*:stack/ApplicationInsights*/*"
      ]
```

```
    },
    {
      "Sid" : "Ec2Actions2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/LaunchWizard-*/*"
        }
      }
    },
    {
      "Sid" : "IamActions0",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:AddRoleToInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonEC2RoleForLaunchWizard*",
        "arn:aws:iam::*:instance-profile/LaunchWizard*"
      ]
    },
    {
      "Sid" : "IamActions1",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonEC2RoleForLaunchWizard",
        "arn:aws:iam::*:role/service-role/AmazonLambdaRoleForLaunchWizard",
        "arn:aws:iam::*:instance-profile/LaunchWizard*"
      ],
      "Condition" : {
        "StringEqualsIfExists" : {
          "iam:PassedToService" : [
```

```
            "lambda.amazonaws.com",
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Sid" : "AutoScalingActions0",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:AttachInstances",
        "autoscaling:CreateAutoScalingGroup",
        "autoscaling:CreateLaunchConfiguration",
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:DeleteLaunchConfiguration",
        "autoscaling:UpdateAutoScalingGroup",
        "autoscaling:CreateOrUpdateTags",
        "resource-groups:CreateGroup",
        "resource-groups:DeleteGroup",
        "sns:ListSubscriptionsByTopic",
        "sns:Publish",
        "ssm:DeleteDocument",
        "ssm:DeleteParameter*",
        "ssm:DescribeDocument*",
        "ssm:GetDocument",
        "ssm:PutParameter"
      ],
      "Resource" : [
        "arn:aws:resource-groups:*:*:group/LaunchWizard*",
        "arn:aws:sns:*:*:*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/
LaunchWizard*",
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/
LaunchWizard*",
        "arn:aws:ssm:*:*:parameter/LaunchWizard*",
        "arn:aws:ssm:*:*:document/LaunchWizard*"
      ]
    },
    {
      "Sid" : "SsmActions0",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetDocument",
```

```
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ssm:*::document/AWS-RunShellScript"
      ]
    },
    {
      "Sid" : "SsmActions1",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/LaunchWizard-*/*"
        }
      }
    },
    {
      "Sid" : "SsmActions2",
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource",
        "ssm:DescribeDocument",
        "ssm:GetDocument",
        "ssm:ListTagsForResource",
        "ssm:RemoveTagsFromResource"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/LaunchWizard*",
        "arn:aws:ssm:*:*:document/LaunchWizard*"
      ]
    },
    {
      "Sid" : "SsmActions3",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:Describe*",
        "cloudformation:DescribeAccountLimits",
        "cloudformation:DescribeStackDriftDetectionStatus",
```

```
        "cloudformation:List*",
        "cloudformation:ValidateTemplate",
        "ds:Describe*",
        "ds:ListAuthorizedApplications",
        "ec2:Describe*",
        "ec2:Get*",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:GetUser",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:List*",
        "resource-groups:Get*",
        "resource-groups:List*",
        "servicequotas:GetServiceQuota",
        "servicequotas:ListServiceQuotas",
        "sns:ListSubscriptions",
        "sns:ListTopics",
        "ssm:CreateDocument",
        "ssm:DescribeAutomation*",
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeParameters",
        "ssm:GetAutomationExecution",
        "ssm:GetCommandInvocation",
        "ssm:GetParameter*",
        "ssm:GetConnectionStatus",
        "ssm:ListCommand*",
        "ssm:ListDocument*",
        "ssm:ListInstanceAssociations",
        "ssm:SendAutomationSignal",
        "tag:Get*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SsmActions4",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution",
        "ssm:StopAutomationExecution"
      ],
      "Resource" : "arn:aws:ssm:*:*:automation-definition/LaunchWizard-*:*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
```

```
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudFormationActions1",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:List*",
        "cloudformation:Describe*"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/LaunchWizard*/"
    },
    {
      "Sid" : "IamActions2",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "autoscaling.amazonaws.com",
            "application-insights.amazonaws.com",
            "events.amazonaws.com",
            "autoscaling.amazonaws.com.cn",
            "events.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Sid" : "LaunchWizardActions0",
      "Effect" : "Allow",
      "Action" : "launchwizard:*",
      "Resource" : "*"
    },
    {
      "Sid" : "SqsActions0",
      "Effect" : "Allow",
      "Action" : [
        "sqs:TagQueue",
        "sqs:GetQueueUrl",
```

```
        "sqs:AddPermission",
        "sqs:ListQueues",
        "sqs:DeleteQueue",
        "sqs:GetQueueAttributes",
        "sqs:ListQueueTags",
        "sqs:CreateQueue",
        "sqs:SetQueueAttributes"
      ],
      "Resource" : "arn:aws:sqs:*:*:LaunchWizard*"
    },
    {
      "Sid" : "CloudWatchActions1",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "iam:GetInstanceProfile",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:LaunchWizard*",
        "arn:aws:iam::*:instance-profile/LaunchWizard*"
      ]
    },
    {
      "Sid" : "EfsActions0",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "route53:ListHostedZones",
        "ec2:CreateSecurityGroup",
        "ec2:AuthorizeSecurityGroupIngress",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:CreateFileSystem",
        "elasticfilesystem:CreateMountTarget",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeMountTargetSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3Actions1",
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::launchwizard*",
        "arn:aws:s3:::launchwizard*/*",
        "arn:aws:s3:::aws-sap-data-provider/config.properties"
      ]
    },
    {
      "Sid" : "CloudFormationActions2",
      "Effect" : "Allow",
      "Action" : "cloudformation:TagResource",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "LaunchWizard*"
        }
      }
    },
    {
      "Sid" : "LambdaActions0",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutBucketVersioning",
        "s3:DeleteBucket",
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:LaunchWizard*",
        "arn:aws:s3:::launchwizard*"
      ]
    },
    {
      "Sid" : "DynamodbActions0",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:CreateTable",
        "dynamodb:DescribeTable",
```

```
        "dynamodb:DeleteTable"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/LaunchWizard*"
    },
    {
      "Sid" : "SecretsManagerActions0",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:TagResource",
        "secretsmanager:UntagResource",
        "secretsmanager:PutResourcePolicy",
        "secretsmanager:DeleteResourcePolicy",
        "secretsmanager:ListSecretVersionIds",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:LaunchWizard*"
    },
    {
      "Sid" : "SecretsManagerActions1",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetRandomPassword",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SsmActions5",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateOpsMetadata"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SsmActions6",
      "Effect" : "Allow",
      "Action" : "ssm:DeleteOpsMetadata",
      "Resource" : "arn:aws:ssm:*:*:opsmetadata/aws/ssm/LaunchWizard*"
    },
    {
      "Sid" : "SnsActions0",
```

```
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:DeleteTopic",
        "sns:Subscribe",
        "sns:Unsubscribe"
      ],
      "Resource" : "arn:aws:sns:*:*:LaunchWizard*"
    },
    {
      "Sid" : "FsxActions0",
      "Effect" : "Allow",
      "Action" : [
        "fsx:UntagResource",
        "fsx:TagResource",
        "fsx:DeleteFileSystem",
        "fsx:ListTagsForResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/Name" : "LaunchWizard*"
        }
      }
    },
    {
      "Sid" : "FsxActions1",
      "Effect" : "Allow",
      "Action" : [
        "fsx:CreateFileSystem"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/Name" : [
            "LaunchWizard*"
          ]
        }
      }
    },
    {
      "Sid" : "FsxActions2",
      "Effect" : "Allow",
      "Action" : [
```

```
        "fsx:DescribeFileSystems"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ServiceCatalogActions0",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:CreatePortfolio",
        "servicecatalog:DescribePortfolio",
        "servicecatalog:CreateConstraint",
        "servicecatalog:CreateProduct",
        "servicecatalog:AssociatePrincipalWithPortfolio",
        "servicecatalog:CreateProvisioningArtifact",
        "servicecatalog:TagResource",
        "servicecatalog:UntagResource"
      ],
      "Resource" : [
        "arn:aws:servicecatalog:*:*:*/*",
        "arn:aws:catalog:*:*:*/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SsmActions7",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:DeleteAssociation"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-ConfigureAWSPackage",
        "arn:aws:ssm:*:*:association/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
```

```
    {
      "Sid" : "EfsActions1",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:UntagResource",
        "elasticfilesystem:TagResource"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "LogsActions0",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DeleteLogGroup",
        "logs:DescribeLogStreams",
        "logs:UntagResource",
        "logs:TagResource",
        "logs:CreateLogGroup",
        "logs:DeleteLogStream",
        "logs:PutLogEvents",
        "logs:GetLogEvents",
        "logs:GetLogDelivery",
        "logs:GetLogGroupFields",
        "logs:GetLogRecord",
        "logs:ListLogDeliveries"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:LaunchWizard*",
        "arn:aws:logs:*:*:log-group:LaunchWizard*:log-stream:*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "LogsActions1",
```

```
      "Effect" : "Allow",
      "Action" : "logs:DescribeLogGroups",
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "FsxActions3",
      "Effect" : "Allow",
      "Action" : [
        "fsx:CreateStorageVirtualMachine",
        "fsx:CreateVolume"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/LaunchWizard-*/*"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "launchwizard.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "FsxActions4",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeStorageVirtualMachines",
        "fsx:DescribeVolumes"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "launchwizard.amazonaws.com"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "FsxActions5",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DeleteStorageVirtualMachine",
        "fsx:DeleteVolume"
      ],
      "Resource" : [
        "arn:aws:fsx:*:*:storage-virtual-machine/*/*",
        "arn:aws:fsx:*:*:backup/*",
        "arn:aws:fsx:*:*:volume/*/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/aws:cloudformation:stack-id" :
 "arn:aws:cloudformation:*:*:stack/LaunchWizard-*/*"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "launchwizard.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonLexChannelsAccess

Deskripsi: Kebijakan ini memungkinkan pelanggan untuk memanggil Lex runtime dari saluran

`AmazonLexChannelsAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 13 Januari 2021 20:12 UTC
- Waktu yang telah diedit: 13 Januari 2021 20:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonLexChannelsAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM

- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonLexFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Lex melalui AWS Management Console. Juga menyediakan akses untuk membuat Peran Tertaut Layanan Lex dan memberikan izin Lex untuk memanggil serangkaian fungsi Lambda terbatas.

`AmazonLexFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonLexFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 11 April 2017, 23:20 UTC
- Waktu yang telah diedit: April 16, 2024, 20:06 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLexFullAccess`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonLexFullAccessStatement1",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
```

```
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "kms:DescribeKey",
        "kms:ListAliases",
        "lambda:GetPolicy",
        "lambda:ListFunctions",
        "lex:*",
        "polly:DescribeVoices",
        "polly:SynthesizeSpeech",
        "kendra:ListIndices",
        "iam:ListRoles",
        "s3:ListAllMyBuckets",
        "logs:DescribeLogGroups",
        "s3:GetBucketLocation"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AmazonLexFullAccessStatement2",
      "Effect" : "Allow",
      "Action" : [
        "lambda:AddPermission",
        "lambda:RemovePermission"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:AmazonLex*",
      "Condition" : {
        "StringEquals" : {
          "lambda:Principal" : "lex.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement3",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/lex.amazonaws.com/
AWSServiceRoleForLexBots",
        "arn:aws:iam::*:role/aws-service-role/channels.lex.amazonaws.com/
AWSServiceRoleForLexChannels",
```

```
        "arn:aws:iam::*:role/aws-service-role/lexv2.amazonaws.com/
AWSServiceRoleForLexV2Bots*",
        "arn:aws:iam::*:role/aws-service-role/channels.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Channels*",
        "arn:aws:iam::*:role/aws-service-role/replication.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Replication*"
      ]
    },
    {
      "Sid" : "AmazonLexFullAccessStatement4",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/lex.amazonaws.com/
AWSServiceRoleForLexBots"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "lex.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement5",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/channels.lex.amazonaws.com/
AWSServiceRoleForLexChannels"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "channels.lex.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement6",
      "Effect" : "Allow",
      "Action" : [
```

```
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/lexv2.amazonaws.com/
AWSServiceRoleForLexV2Bots*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "lexv2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement7",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/channels.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Channels*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "channels.lexv2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement8",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/replication.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Replication*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "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"
```

```
            ]
          }
        }
      }
    ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonLexReadOnly

Deskripsi: Menyediakan akses hanya-baca ke Amazon Lex.

`AmazonLexReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonLexReadOnly` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 11 April 2017, 23:13 UTC
- Waktu yang telah diedit: 13 Mei 2024, 16:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLexReadOnly`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonLexReplicationPolicy

Deskripsi: Memungkinkan Amazon Lex untuk mereplikasi sumber daya Lex di seluruh wilayah atas nama Anda.

`AmazonLexReplicationPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 31 Januari 2024, 23:29 UTC
- Waktu yang telah diedit: 24 Juni 2025, 21:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonLexReplicationPolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReplicationServicePolicyStatement1",
      "Effect" : "Allow",
      "Action" : [
        "lex:BuildBotLocale",
        "lex:ListBotLocales",
        "lex:CreateBotAlias",
        "lex:UpdateBotAlias",
        "lex:DeleteBotAlias",
        "lex:DescribeBotAlias",
        "lex:CreateBotVersion",
        "lex:DeleteBotVersion",
        "lex:DescribeBotVersion",
        "lex:CreateExport",
```

```
        "lex:DescribeBot",
        "lex:UpdateExport",
        "lex:DescribeExport",
        "lex:DescribeBotLocale",
        "lex:DescribeIntent",
        "lex:ListIntents",
        "lex:DescribeSlotType",
        "lex:ListSlotTypes",
        "lex:DescribeSlot",
        "lex:ListSlots",
        "lex:DescribeCustomVocabulary",
        "lex:StartImport",
        "lex:DescribeImport",
        "lex:CreateBot",
        "lex:UpdateBot",
        "lex:DeleteBot",
        "lex:CreateBotLocale",
        "lex:UpdateBotLocale",
        "lex:DeleteBotLocale",
        "lex:CreateIntent",
        "lex:UpdateIntent",
        "lex:DeleteIntent",
        "lex:CreateSlotType",
        "lex:UpdateSlotType",
        "lex:DeleteSlotType",
        "lex:CreateSlot",
        "lex:UpdateSlot",
        "lex:DeleteSlot",
        "lex:CreateCustomVocabulary",
        "lex:UpdateCustomVocabulary",
        "lex:DeleteCustomVocabulary",
        "lex:DeleteBotChannel",
        "lex: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"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonLexRunBotsOnly

Deskripsi: Menyediakan akses ke percakapan APIs Amazon Lex.

`AmazonLexRunBotsOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonLexRunBotsOnly` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 11 April 2017, 23:06 UTC
- Waktu yang telah diedit: 18 Agustus 2021, 00:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLexRunBotsOnly`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lex:PostContent",
        "lex:PostText",
        "lex:PutSession",
        "lex:GetSession",
        "lex:DeleteSession",
        "lex:RecognizeText",
```

```
        "lex:RecognizeUtterance",
        "lex:StartConversation"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonLexV2BotPolicy

Deskripsi: Menyediakan Lex V2 bot akses untuk memanggil AWS layanan lain atas nama Anda.

`AmazonLexV2BotPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 13 Januari 2021 20:10 UTC
- Waktu yang telah diedit: 13 Januari 2021, 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonLexV2BotPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonLookoutEquipmentFullAccess

Deskripsi: Menyediakan akses penuh ke operasi Amazon Lookout for Equipment

`AmazonLookoutEquipmentFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonLookoutEquipmentFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 08 April 2021, 15:52 UTC
- Waktu yang telah diedit: 24 November 2021, 21:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutEquipmentFullAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lookoutequipment:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lookoutequipment.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "lookoutequipment.*.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonLookoutEquipmentReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon Lookout for Equipments

`AmazonLookoutEquipmentReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonLookoutEquipmentReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 05 Mei 2021 16:47 UTC
- Waktu yang telah diedit: 10 November 2022, 22.04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutEquipmentReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonLookoutMetricsFullAccess

Deskripsi: Memberikan akses ke semua tindakan untuk Amazon Lookout for Metrics

`AmazonLookoutMetricsFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonLookoutMetricsFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 07 Mei 2021 00:43 UTC
- Waktu yang telah diedit: 07 Mei 2021, 00:43 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutMetricsFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonLookoutMetricsReadOnlyAccess

Deskripsi: Memberikan akses ke semua tindakan hanya-baca untuk Amazon Lookout for Metrics

`AmazonLookoutMetricsReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonLookoutMetricsReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 07 Mei 2021 00:43 UTC
- Waktu yang telah diedit: 04 Januari 2022, 18.19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutMetricsReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lookoutmetrics:DescribeMetricSet",
        "lookoutmetrics:ListMetricSets",
        "lookoutmetrics:DescribeAnomalyDetector",
        "lookoutmetrics:ListAnomalyDetectors",
        "lookoutmetrics:DescribeAnomalyDetectionExecutions",
        "lookoutmetrics:DescribeAlert",
        "lookoutmetrics:ListAlerts",
        "lookoutmetrics:ListTagsForResource",
        "lookoutmetrics:ListAnomalyGroupSummaries",
        "lookoutmetrics:ListAnomalyGroupTimeSeries",
        "lookoutmetrics:ListAnomalyGroupRelatedMetrics",
        "lookoutmetrics:GetAnomalyGroup",
        "lookoutmetrics:GetDataQualityMetrics",
        "lookoutmetrics:GetSampleData",
        "lookoutmetrics:GetFeedback"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonLookoutVisionConsoleFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Lookout for Vision dan akses cakupan ke dependensi layanan dan konsol yang diperlukan.

`AmazonLookoutVisionConsoleFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonLookoutVisionConsoleFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 11 Mei 2021 19:37 UTC
- Waktu yang telah diedit: 11 Mei 2021 19:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutVisionConsoleFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      "Action" : [
        "lookoutvision:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LookoutVisionConsoleS3BucketSearchAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LookoutVisionConsoleS3BucketFirstUseSetupAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutBucketVersioning",
        "s3:PutLifecycleConfiguration",
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketPublicAccessBlock"
      ],
      "Resource" : "arn:aws:s3:::lookoutvision-*"
    },
    {
      "Sid" : "LookoutVisionConsoleS3BucketAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:GetBucketVersioning"
      ],
      "Resource" : "arn:aws:s3:::lookoutvision-*"
    },
    {
      "Sid" : "LookoutVisionConsoleS3ObjectAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:PutObject",
        "s3:AbortMultipartUpload",
        "s3:ListMultipartUploadParts"
```

```
      ],
      "Resource" : "arn:aws:s3:::lookoutvision-*/*"
    },
    {
      "Sid" : "LookoutVisionConsoleDatasetLabelingToolsAccess",
      "Effect" : "Allow",
      "Action" : [
        "groundtruthlabeling:RunGenerateManifestByCrawlingJob",
        "groundtruthlabeling:AssociatePatchToManifestJob",
        "groundtruthlabeling:DescribeConsoleJob"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LookoutVisionConsoleDashboardAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LookoutVisionConsoleTagSelectorAccess",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetTagKeys",
        "tag:GetTagValues"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LookoutVisionConsoleKmsKeySelectorAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonLookoutVisionConsoleReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon Lookout for Vision dan akses cakupan ke dependensi layanan dan konsol yang diperlukan.

`AmazonLookoutVisionConsoleReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonLookoutVisionConsoleReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 11 Mei 2021 19:32 UTC
- Waktu yang telah diedit: 09 Desember 2021 02:46 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutVisionConsoleReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LookoutVisionReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "lookoutvision:DescribeDataset",
        "lookoutvision:DescribeModel",
        "lookoutvision:DescribeProject",
        "lookoutvision:DescribeTrialDetection",
        "lookoutvision:DescribeModelPackagingJob",
        "lookoutvision:ListDatasetEntries",
        "lookoutvision:ListModels",
        "lookoutvision:ListProjects",
        "lookoutvision:ListTagsForResource",
        "lookoutvision:ListTrialDetections",
        "lookoutvision:ListModelPackagingJobs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LookoutVisionConsoleS3BucketSearchAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LookoutVisionConsoleS3ObjectReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::lookoutvision-*/*"
    },
    {
      "Sid" : "LookoutVisionConsoleDashboardAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics"
      ],
```

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonLookoutVisionFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Lookout for Vision dan akses cakupan ke dependensi yang diperlukan.

`AmazonLookoutVisionFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonLookoutVisionFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 11 Mei 2021 19:24 UTC
- Waktu yang telah diedit: 11 Mei 2021 19.24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutVisionFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonLookoutVisionReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon Lookout for Vision dan akses cakupan ke dependensi yang diperlukan.

`AmazonLookoutVisionReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonLookoutVisionReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 11 Mei 2021 19:11 UTC
- Waktu telah diedit: 09 Desember 2021 03:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutVisionReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LookoutVisionReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "lookoutvision:DescribeDataset",
        "lookoutvision:DescribeModel",
        "lookoutvision:DescribeProject",
        "lookoutvision:DescribeModelPackagingJob",
        "lookoutvision:ListDatasetEntries",
        "lookoutvision:ListModels",
        "lookoutvision:ListProjects",
        "lookoutvision:ListTagsForResource",
        "lookoutvision:ListModelPackagingJobs"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonMachineLearningBatchPredictionsAccess

Deskripsi: Memberikan izin kepada pengguna untuk meminta prediksi batch Amazon Machine Learning.

`AmazonMachineLearningBatchPredictionsAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonMachineLearningBatchPredictionsAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 09 April 2015, 17:12 UTC
- Waktu telah diedit: 09 April 2015, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningBatchPredictionsAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:CreateBatchPrediction",
        "machinelearning:DeleteBatchPrediction",
        "machinelearning:DescribeBatchPredictions",
        "machinelearning:GetBatchPrediction",
        "machinelearning:UpdateBatchPrediction"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonMachineLearningCreateOnlyAccess

Deskripsi: Menyediakan akses buat untuk sumber daya Amazon Machine Learning non-prediksi.

`AmazonMachineLearningCreateOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonMachineLearningCreateOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 09 April 2015, 17:18 UTC
- Waktu telah diedit: 29 Juni 2016, 20:55 UTC

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

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:Add*",
        "machinelearning:Create*",
        "machinelearning:Delete*",
        "machinelearning:Describe*",
        "machinelearning:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonMachineLearningFullAccess

Deskripsi: Menyediakan akses penuh ke sumber daya Amazon Machine Learning.

`AmazonMachineLearningFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonMachineLearningFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 09 April 2015, 17:25 UTC
- Waktu telah diedit: 09 April 2015, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonMachineLearningManageRealTimeEndpointOnlyAccess

Deskripsi: Memberikan izin kepada pengguna untuk membuat dan menghapus titik akhir real-time untuk model Amazon Machine Learning.

`AmazonMachineLearningManageRealTimeEndpointOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonMachineLearningManageRealTimeEndpointOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 09 April 2015, 17:32 UTC
- Waktu telah diedit: 09 April 2015, 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningManageRealTimeEndpointOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonMachineLearningReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke sumber daya Amazon Machine Learning.

`AmazonMachineLearningReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonMachineLearningReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 09 April 2015, 17:40 UTC

- Waktu telah diedit: 09 April 2015, 17:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonMachineLearningRealTimePredictionOnlyAccess

Deskripsi: Memberikan izin kepada pengguna untuk meminta prediksi real-time Amazon Machine Learning.

`AmazonMachineLearningRealTimePredictionOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonMachineLearningRealTimePredictionOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 09 April 2015, 17:44 UTC
- Waktu telah diedit: 09 April 2015, 17:44 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningRealTimePredictionOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonMachineLearningRoleforRedshiftDataSourceV3

Deskripsi: Memungkinkan Machine Learning mengonfigurasi dan menggunakan Redshift Clusters dan Staging Locations S3 untuk Sumber Data Redshift.

`AmazonMachineLearningRoleforRedshiftDataSourceV3`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonMachineLearningRoleforRedshiftDataSourceV3` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 24 Juni 2020, 18:00 UTC
- Waktu yang telah diedit: 24 Juni 2020, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonMachineLearningRoleforRedshiftDataSourceV3`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupIngress",
        "redshift:AuthorizeClusterSecurityGroupIngress",
        "redshift:CreateClusterSecurityGroup",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSecurityGroups",
        "redshift:ModifyCluster",
        "redshift:RevokeClusterSecurityGroupIngress"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketPolicy",
        "s3:GetBucketLocation",
        "s3:GetBucketPolicy",
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::amazon-machine-learning*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonMacieFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Macie.

`AmazonMacieFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonMacieFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 14 Agustus 2017, 14:54 UTC
- Waktu yang telah diedit: 01 Juli 2022, 00:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMacieFullAccess`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "macie2:*"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/macie.amazonaws.com/
AWSServiceRoleForAmazonMacie",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "macie.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "pricing:GetProducts",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonMacieHandshakeRole

Deskripsi: Memberikan izin untuk membuat peran Amazon Macie terkait layanan.

`AmazonMacieHandshakeRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonMacieHandshakeRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan

- Waktu pembuatan: 28 Juni 2018, 15:46 UTC
- Waktu yang telah diedit: 28 Juni 2018, 15:46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonMacieHandshakeRole`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "iam:AWSServiceName" : "macie.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonMacieReadOnlyAccess

Deskripsi: Menyediakan akses readonly ke Amazon Macie.

`AmazonMacieReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonMacieReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 15 Juni 2023, 21:50 UTC
- Waktu yang telah diedit: 15 Juni 2023, 21:50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMacieReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "macie2:Describe*",
        "macie2:Get*",
        "macie2:List*",
        "macie2:BatchGetCustomDataIdentifiers",
        "macie2:SearchResources"
      ],
```

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonMacieServiceRole

Deskripsi: Memberikan Macie akses hanya-baca ke dependensi sumber daya di akun Anda untuk mengaktifkan analisis data.

`AmazonMacieServiceRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonMacieServiceRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 14 Agustus 2017, 14:53 UTC
- Waktu yang telah diedit: 14 Agustus 2017, 14:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonMacieServiceRole`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "s3:Get*",
        "s3:List*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonMacieServiceRolePolicy

Deskripsi: Peran terkait layanan untuk Amazon Macie

`AmazonMacieServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 19 Juni 2018, 22:17 UTC

- Waktu yang telah diedit: 19 Mei 2022 19.16 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonMacieServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListAccountAliases",
        "organizations:DescribeAccount",
        "organizations:ListAccounts",
        "s3:GetAccountPublicAccessBlock",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "s3:GetBucketWebsite",
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetReplicationConfiguration",
        "s3:ListBucket",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectTagging"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/macie/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/macie/*:log-stream:*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonManagedBlockchainConsoleFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Managed Blockchain melalui AWS Management Console

`AmazonManagedBlockchainConsoleFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonManagedBlockchainConsoleFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 April 2019, 21:23 UTC
- Waktu yang telah diedit: 29 April 2019, 21:23 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonManagedBlockchainConsoleFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "managedblockchain:*",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:CreateVpcEndpoint",
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonManagedBlockchainFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Managed Blockchain.

`AmazonManagedBlockchainFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonManagedBlockchainFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 April 2019, 21:39 UTC
- Waktu yang telah diedit: 29 April 2019, 21:39 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonManagedBlockchainFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonManagedBlockchainReadOnlyAccess

Deskripsi: Menyediakan akses hanya-baca ke Amazon Managed Blockchain.

`AmazonManagedBlockchainReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonManagedBlockchainReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 30 April 2019, 18:17 UTC
- Waktu yang telah diedit: 30 April 2019, 18:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonManagedBlockchainReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonManagedBlockchainServiceRolePolicy

Deskripsi: Mengaktifkan akses ke Layanan AWS dan Sumber Daya yang digunakan atau dikelola oleh Amazon Managed Blockchain

`AmazonManagedBlockchainServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 17 Januari 2020, 19:51 UTC
- Waktu yang telah diedit: 17 Januari 2020, 19:51 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonManagedBlockchainServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/managedblockchain/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/managedblockchain/*:log-stream:*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonMCSFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Managed Apache Cassandra Service

`AmazonMCSFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonMCSFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 Desember 2019, 13:45 UTC
- Waktu yang telah diedit: 17 April 2020, 19:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMCSFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget",
        "application-autoscaling:PutScheduledAction",
        "application-autoscaling:DeleteScheduledAction",
        "application-autoscaling:DescribeScheduledActions"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cassandra:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:PutMetricAlarm"
      ],
```

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonMCSReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon Managed Apache Cassandra Service

`AmazonMCSReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonMCSReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 Desember 2019, 13:46 UTC
- Waktu yang telah diedit: 17 April 2020, 19:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMCSReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cassandra:Select"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonMechanicalTurkFullAccess

Deskripsi: Menyediakan akses penuh ke semua APIs di Amazon Mechanical Turk.

`AmazonMechanicalTurkFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonMechanicalTurkFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 11 Desember 2015, 19:08 UTC
- Waktu telah diedit: 11 Desember 2015, 19:08 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMechanicalTurkFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonMechanicalTurkReadOnly

Deskripsi: Menyediakan akses untuk membaca hanya APIs di Amazon Mechanical Turk.

`AmazonMechanicalTurkReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonMechanicalTurkReadOnly` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 11 Desember 2015, 19:08 UTC
- Waktu yang telah diedit: 25 September 2019, 21:06 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMechanicalTurkReadOnly`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonMemoryDBFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon MemoryDB melalui file. AWS Management Console

`AmazonMemoryDBFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonMemoryDBFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 08 Oktober 2021 19:24 UTC

- Waktu yang telah diedit: 08 Oktober 2021 19:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMemoryDBFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonMemoryDBReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon MemoryDB melalui file. AWS Management Console

`AmazonMemoryDBReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonMemoryDBReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 08 Oktober 2021 19:27 UTC
- Waktu yang telah diedit: 08 Oktober 2021 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMemoryDBReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
        "memorydb:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonMobileAnalyticsFinancialReportAccess

Deskripsi: Menyediakan akses baca saja ke semua laporan termasuk data keuangan untuk semua sumber daya aplikasi.

`AmazonMobileAnalyticsFinancialReportAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonMobileAnalyticsFinancialReportAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu telah diedit: 06 Februari 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMobileAnalyticsFinancialReportAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonMobileAnalyticsFullAccess

Deskripsi: Menyediakan akses penuh ke semua sumber daya aplikasi.

`AmazonMobileAnalyticsFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonMobileAnalyticsFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu telah diedit: 06 Februari 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMobileAnalyticsFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonMobileAnalyticsNon-financialReportAccess

Deskripsi: Menyediakan akses baca saja ke laporan non keuangan untuk semua sumber daya aplikasi.

`AmazonMobileAnalyticsNon-financialReportAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonMobileAnalyticsNon-financialReportAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu telah diedit: 06 Februari 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMobileAnalyticsNon-financialReportAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonMobileAnalyticsWriteOnlyAccess

Deskripsi: Menyediakan akses tulis saja untuk menempatkan data peristiwa untuk semua sumber daya aplikasi. (Direkomendasikan untuk integrasi SDK)

`AmazonMobileAnalyticsWriteOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonMobileAnalyticsWriteOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu telah diedit: 06 Februari 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMobileAnalyticsWriteOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonMonitronFullAccess

Deskripsi: Menyediakan akses penuh untuk mengelola Amazon Monitron

`AmazonMonitronFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonMonitronFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 02 Desember 2020, 22:40 UTC
- Waktu yang telah diedit: 08 Juni 2022, 16.27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMonitronFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "monitron.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "monitron:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "*",
```

```
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "monitron.*.amazonaws.com"
          ]
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        }
      }
    },
    {
      "Sid" : "AWSSSOPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "ds:DescribeDirectories",
        "ds:DescribeTrusts"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:DescribeStream",
        "kinesis:ListStreams"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/monitron/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonMQApiFullAccess

Deskripsi: Menyediakan akses penuh ke AmazonMQ melalui API/SDK kami.

`AmazonMQApiFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonMQApiFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 Desember 2018, 20:31 UTC
- Waktu yang telah diedit: 04 November 2020, 16:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMQApiFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      "Effect" : "Allow",
      "Action" : [
        "mq:*",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DetachNetworkInterface",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/amazonmq/*"
      ]
    },
    {
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "mq.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonMQApiReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke AmazonMQ melalui API/SDK kami.

`AmazonMQApiReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonMQApiReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 Desember 2018, 20:31 UTC
- Waktu telah diedit: 18 Desember 2018, 20:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMQApiReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonMQFullAccess

Deskripsi: Menyediakan akses penuh ke AmazonMQ melalui. AWS Management Console

`AmazonMQFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonMQFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 November 2017, 15:28 UTC
- Waktu yang telah diedit: 04 November 2020, 16:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMQFullAccess`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mq:*",
        "cloudformation:CreateStack",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DetachNetworkInterface",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:CreateSecurityGroup",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/amazonmq/*"
      ]
    },
    {
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
```

```
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "mq.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin dengan hak istimewa paling sedikit

AmazonMQReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke AmazonMQ melalui. AWS Management Console

`AmazonMQReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonMQReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 November 2017, 15:30 UTC
- Waktu telah diedit: 28 November 2017, 19:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMQReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mq:Describe*",
        "mq:List*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonMQServiceRolePolicy

Deskripsi: Kebijakan Peran Tertaut Layanan untuk AWS Amazon MQ

`AmazonMQServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 04 November 2020, 16:07 UTC
- Waktu yang telah diedit: 04 November 2020, 16:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonMQServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
```

```
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AMQManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AMQManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "logs:PutLogEvents",
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups",
        "logs:CreateLogStream",
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/amazonmq/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonMSKConnectReadOnlyAccess

Deskripsi: Menyediakan akses readonly ke Amazon MSK Connect

`AmazonMSKConnectReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonMSKConnectReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 20 September 2021 10:18 UTC
- Waktu telah diedit: 18 Oktober 2021 09:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMSKConnectReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kafkaconnect:ListConnectors",
        "kafkaconnect:ListCustomPlugins",
        "kafkaconnect:ListWorkerConfigurations"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kafkaconnect:DescribeConnector"
      ],
      "Resource" : [
        "arn:aws:kafkaconnect:*:*:connector/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kafkaconnect:DescribeCustomPlugin"
      ],
      "Resource" : [
        "arn:aws:kafkaconnect:*:*:custom-plugin/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "kafkaconnect:DescribeWorkerConfiguration"
      ],
      "Resource" : [
        "arn:aws:kafkaconnect:*:*:worker-configuration/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonMSKFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon MSK dan izin lain yang diperlukan untuk dependensinya.

`AmazonMSKFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonMSKFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 14 Januari 2019, 22:07 UTC
- Waktu telah diedit: 18 Oktober 2023, 11:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMSKFullAccess`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kafka:*",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcAttribute",
        "kms:DescribeKey",
        "kms:CreateGrant",
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries",
        "logs:PutResourcePolicy",
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups",
        "S3:GetBucketPolicy",
        "firehose:TagDeliveryStream"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:*:ec2:*:*:vpc/*",
        "arn:*:ec2:*:*:subnet/*",
        "arn:*:ec2:*:*:security-group/*"
```

```
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:*:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AWSMSKManaged" : "true"
        },
        "StringLike" : {
          "aws:RequestTag/ClusterArn" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:*:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "arn:*:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AWSMSKManaged" : "true"
        },
        "StringLike" : {
          "ec2:ResourceTag/ClusterArn" : "*"
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "kafka.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/kafka.amazonaws.com/
AWSServiceRoleForKafka*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "kafka.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/delivery.logs.amazonaws.com/
AWSServiceRoleForLogDelivery*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "delivery.logs.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonMSKReadOnlyAccess

Deskripsi: Menyediakan akses readonly ke Amazon MSK

`AmazonMSKReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonMSKReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 14 Januari 2019, 22:28 UTC
- Waktu yang telah diedit: 14 Januari 2019, 22:28 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMSKReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "kafka:Describe*",
        "kafka:List*",
        "kafka:Get*",
        "ec2:DescribeNetworkInterfaces",
```

```
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "kms:DescribeKey"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonMWAAServiceRolePolicy

Deskripsi: Peran Tertaut Layanan yang digunakan oleh Alur Kerja Terkelola Amazon untuk Apache Airflow.

`AmazonMWAAServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 24 November 2020, 14:13 UTC
- Waktu yang telah diedit: 17 November 2022 00:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonMWAAServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:airflow-*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachNetworkInterface",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ec2:DetachNetworkInterface"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
```

```
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "AmazonMWAAManaged"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint",
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonMWAAManaged" : false
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "AmazonMWAAManaged"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/MWAA"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonNimbleStudio-LaunchProfileWorker

Deskripsi: Kebijakan ini memberikan akses ke sumber daya yang dibutuhkan oleh pekerja Profil Peluncuran Studio Nimble. Lampirkan kebijakan ini ke EC2 instance yang dibuat oleh Nimble Studio Builder.

`AmazonNimbleStudio-LaunchProfileWorker`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonNimbleStudio-LaunchProfileWorker` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 April 2021, 04:47 UTC
- Waktu yang telah diedit: 28 April 2021, 04:47 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonNimbleStudio-LaunchProfileWorker`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "fsx:DescribeFileSystems",
        "ds:DescribeDirectories"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "nimble.amazonaws.com"
        }
      },
      "Sid" : "GetLaunchProfileInitializationDependencies"
    }
  ],
  "Version" : "2012-10-17"
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonNimbleStudio-StudioAdmin

Deskripsi: Kebijakan ini memberikan akses ke sumber daya Amazon Nimble Studio yang terkait dengan admin studio dan sumber daya studio terkait di layanan lain. Lampirkan kebijakan ini ke peran Admin yang terkait dengan studio Anda.

`AmazonNimbleStudio-StudioAdmin`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonNimbleStudio-StudioAdmin` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 April 2021, 04:47 UTC
- Waktu telah diedit: September 22, 2023, 17:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonNimbleStudio-StudioAdmin`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Statement" : [
    {
      "Sid" : "StudioAdminFullAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "nimble:CreateStreamingSession",
        "nimble:GetStreamingSession",
        "nimble:StartStreamingSession",
        "nimble:StopStreamingSession",
        "nimble:CreateStreamingSessionStream",
        "nimble:GetStreamingSessionStream",
        "nimble:DeleteStreamingSession",
        "nimble:ListStreamingSessionBackups",
        "nimble:GetStreamingSessionBackup",
        "nimble:ListEulas",
        "nimble:ListEulaAcceptances",
        "nimble:GetEula",
        "nimble:AcceptEulas",
        "nimble:ListStudioMembers",
        "nimble:GetStudioMember",
        "nimble:ListStreamingSessions",
        "nimble:GetStreamingImage",
        "nimble:ListStreamingImages",
        "nimble:GetLaunchProfileInitialization",
        "nimble:GetLaunchProfileDetails",
        "nimble:GetFeatureMap",
        "nimble:PutStudioLogEvents",
        "nimble:ListLaunchProfiles",
        "nimble:GetLaunchProfile",
        "nimble:GetLaunchProfileMember",
        "nimble:ListLaunchProfileMembers",
        "nimble:PutLaunchProfileMembers",
        "nimble:UpdateLaunchProfileMember",
        "nimble:DeleteLaunchProfileMember"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:DescribeUsers",
        "sso-directory:SearchUsers",
        "identitystore:DescribeUser",
        "identitystore:ListUsers"
      ],
      "Resource" : [
        "*"
      ]
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ds:CreateComputer",
        "ds:DescribeDirectories",
        "ec2:DescribeSubnets",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeSecurityGroups",
        "fsx:DescribeFileSystems"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "nimble.amazonaws.com"
        }
      }
    }
  ],
  "Version" : "2012-10-17"
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonNimbleStudio-StudioUser

Deskripsi: Kebijakan ini memberikan akses ke sumber daya Amazon Nimble Studio yang terkait dengan pengguna studio dan sumber daya studio terkait di layanan lain. Lampirkan kebijakan ini ke peran Pengguna yang terkait dengan studio Anda.

`AmazonNimbleStudio-StudioUser`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonNimbleStudio-StudioUser` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 April 2021, 04:48 UTC
- Waktu yang telah diedit: September 22, 2023, 17:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonNimbleStudio-StudioUser`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ds:CreateComputer",
        "ec2:DescribeSubnets",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeSecurityGroups",
        "fsx:DescribeFileSystems",
        "ds:DescribeDirectories"
      ],
```

```
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "nimble.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:DescribeUsers",
        "sso-directory:SearchUsers",
        "identitystore:DescribeUser",
        "identitystore:ListUsers"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "nimble:ListLaunchProfiles"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "nimble:requesterPrincipalId" : "${nimble:principalId}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "nimble:ListStudioMembers",
        "nimble:GetStudioMember",
        "nimble:ListEulas",
        "nimble:ListEulaAcceptances",
        "nimble:GetFeatureMap",
        "nimble:PutStudioLogEvents"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "nimble:DeleteStreamingSession",
        "nimble:GetStreamingSession",
        "nimble:StartStreamingSession",
        "nimble:StopStreamingSession",
        "nimble:CreateStreamingSessionStream",
        "nimble:GetStreamingSessionStream",
        "nimble:ListStreamingSessions",
        "nimble:ListStreamingSessionBackups",
        "nimble:GetStreamingSessionBackup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "nimble:ownedBy" : "${nimble:requesterPrincipalId}"
        }
      }
    }
  ],
  "Version" : "2012-10-17"
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonODBServiceRolePolicy

Deskripsi: Memungkinkan Oracle Database@AWS untuk mengelola AWS sumber daya atas nama Anda.

`AmazonODBServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 13 November 2024, 18:21 UTC
- Waktu yang telah diedit: 03 Juli 2025, 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonODBServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonOmicsFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Omics dan lainnya yang diperlukan Layanan AWS. Kebijakan ini memungkinkan pengguna untuk melihat dan menerima undangan berbagi RAM untuk mengakses sumber daya di luar pengguna. Akun AWS

`AmazonOmicsFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonOmicsFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 24 Februari 2023, 00:59 UTC
- Waktu yang telah diedit: 24 Februari 2023, 00:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOmicsFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      "Effect" : "Allow",
      "Action" : [
        "ram:AcceptResourceShareInvitation",
        "ram:GetResourceShareInvitations"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "omics.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "omics.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonOmicsReadOnlyAccess

Deskripsi: Berikan akses baca saja ke Amazon Omics

`AmazonOmicsReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonOmicsReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 November 2022, 04:17 UTC
- Waktu telah diedit: 29 November 2022, 04:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOmicsReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonOneEnterpriseFullAccess

Deskripsi: Kebijakan ini memberikan izin administratif yang memungkinkan akses ke semua sumber daya dan operasi Amazon One Enterprise.

`AmazonOneEnterpriseFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonOneEnterpriseFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 November 2023, 04:58 UTC
- Waktu telah diedit: 28 November 2023, 04:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOneEnterpriseFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonOneEnterpriseInstallerAccess

Deskripsi: Kebijakan ini memberikan izin baca dan tulis terbatas yang memungkinkan penginstalan dan aktivasi perangkat.

`AmazonOneEnterpriseInstallerAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonOneEnterpriseInstallerAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 November 2023, 05:00 UTC
- Waktu telah diedit: 28 November 2023, 05:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOneEnterpriseInstallerAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "InstallerAccessStatementID",
      "Effect" : "Allow",
      "Action" : [
        "one:CreateDeviceActivationQrCode",
        "one:GetDeviceInstance",
        "one:GetSite",
        "one:GetSiteAddress",
        "one:ListDeviceInstances",
        "one:ListSites"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonOneEnterpriseReadOnlyAccess

Deskripsi: Kebijakan ini memberikan izin baca saja ke semua sumber daya dan operasi Amazon One Enterprise.

`AmazonOneEnterpriseReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonOneEnterpriseReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 November 2023, 04:59 UTC
- Waktu telah diedit: 28 November 2023, 04:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOneEnterpriseReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonOpenSearchDashboardsServiceRolePolicy

Deskripsi: Menyediakan akses ke Layanan OpenSearch Dasbor Amazon untuk mengakses AWS layanan lain seperti CloudWatch atas nama Anda

`AmazonOpenSearchDashboardsServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 22 Desember 2023, 19:38 UTC
- Waktu telah diedit: 22 Desember 2023, 19:38 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchDashboardsServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/AOSD"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonOpenSearchDirectQueryGlueCreateAccess

Deskripsi: Memungkinkan OpenSearch DirectQuery Layanan mengakses AWS Glue APIs untuk membuat sumber daya atas nama Anda.

`AmazonOpenSearchDirectQueryGlueCreateAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonOpenSearchDirectQueryGlueCreateAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Mei 2024, 12:24 UTC
- Waktu yang telah diedit: 06 Mei 2024, 12:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchDirectQueryGlueCreateAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonOpenSearchDirectQueryGlueCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:CreatePartition",
        "glue:CreateTable",
        "glue:BatchCreatePartition"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonOpenSearchIngestionFullAccess

Deskripsi: Memungkinkan Amazon OpenSearch Ingestion mengakses AWS layanan lain atas nama Anda.

`AmazonOpenSearchIngestionFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonOpenSearchIngestionFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 26 April 2023, 18:11 UTC
- Waktu yang telah diedit: 26 April 2023, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchIngestionFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "osis:CreatePipeline",
        "osis:UpdatePipeline",
        "osis:DeletePipeline",
        "osis:StartPipeline",
        "osis:StopPipeline",
        "osis:ListPipelines",
        "osis:GetPipeline",
        "osis:GetPipelineChangeProgress",
        "osis:ValidatePipeline",
        "osis:GetPipelineBlueprint",
        "osis:ListPipelineBlueprints",
        "osis:TagResource",
```

```
        "osis:UntagResource",
        "osis:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/osis.amazonaws.com/
AWSServiceRoleForAmazonOpenSearchIngestionService",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "osis.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonOpenSearchIngestionReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon OpenSearch Ingestion Service

`AmazonOpenSearchIngestionReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonOpenSearchIngestionReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 26 April 2023, 18:09 UTC
- Waktu yang telah diedit: 26 April 2023, 18:09 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchIngestionReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "osis:GetPipeline",
        "osis:GetPipelineChangeProgress",
        "osis:GetPipelineBlueprint",
        "osis:ListPipelineBlueprints",
        "osis:ListPipelines",
        "osis:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonOpenSearchIngestionServiceRolePolicy

Deskripsi: Memungkinkan Amazon OpenSearch Ingestion Service untuk mengakses AWS layanan lain atas nama Anda.

`AmazonOpenSearchIngestionServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 18 November 2022, 16:49 UTC
- Waktu telah diedit: 18 November 2022, 16.49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchIngestionServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
```

```
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/OSISManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/OSISManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/OSIS"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonOpenSearchServerlessServiceRolePolicy

Deskripsi: Izinkan Amazon OpenSearch Tanpa Server mengakses AWS layanan lain seperti CloudWatch APIs atas nama Anda.

`AmazonOpenSearchServerlessServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 24 November 2022, 19:50 UTC
- Waktu yang telah diedit: 25 Juli 2024, 21:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchServerlessServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM

- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonOpenSearchServiceCognitoAccess

Deskripsi: Menyediakan akses ke layanan konfigurasi Amazon Cognito.

`AmazonOpenSearchServiceCognitoAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonOpenSearchServiceCognitoAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 02 September 2021, 06:31 UTC
- Waktu yang telah diedit: 20 Desember 2021 14:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchServiceCognitoAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:DescribeUserPool",
        "cognito-idp:CreateUserPoolClient",
```

```
        "cognito-idp:DeleteUserPoolClient",
        "cognito-idp:UpdateUserPoolClient",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:AdminInitiateAuth",
        "cognito-idp:AdminUserGlobalSignOut",
        "cognito-idp:ListUserPoolClients",
        "cognito-identity:DescribeIdentityPool",
        "cognito-identity:UpdateIdentityPool",
        "cognito-identity:GetIdentityPoolRoles"
      ],
      "Resource" : [
        "arn:aws:cognito-identity:*:*:identitypool/*",
        "arn:aws:cognito-idp:*:*:userpool/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "cognito-identity.amazonaws.com",
            "cognito-identity-us-gov.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "cognito-identity:SetIdentityPoolRoles",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonOpenSearchServiceFullAccess

Deskripsi: Menyediakan akses penuh ke OpenSearch layanan konfigurasi Layanan Amazon.

`AmazonOpenSearchServiceFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonOpenSearchServiceFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 08 September 2021, 05:33 UTC
- Waktu telah diedit: September 08, 2021, 05:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchServiceFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonOpenSearchServiceReadOnlyAccess

Deskripsi: Menyediakan akses hanya-baca ke OpenSearch layanan konfigurasi Layanan Amazon.

`AmazonOpenSearchServiceReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonOpenSearchServiceReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 08 September 2021, 05:38 UTC
- Waktu yang telah diedit: September 08, 2021, 05:38 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchServiceReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonOpenSearchServiceRolePolicy

Deskripsi: Izinkan OpenSearch Layanan Amazon mengakses AWS layanan lain seperti EC2 Jaringan APIs atas nama Anda.

`AmazonOpenSearchServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 26 Agustus 2021 09:27 UTC
- Waktu telah diedit: 27 Maret 2025, 22:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Stmt1480452973134",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "Stmt1480452973145",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "Stmt1480452973144",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    },
    {
      "Sid" : "Stmt1480452973165",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "Stmt1480452973149",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignIpv6Addresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*"
    },
    {
      "Sid" : "Stmt1480452973150",
      "Effect" : "Allow",
      "Action" : [
        "ec2:UnAssignIpv6Addresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*"
    },
    {
      "Sid" : "Stmt1480452973154",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSecurityGroups"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973164",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973174",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973184",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddListenerCertificates",
        "elasticloadbalancing:RemoveListenerCertificates"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:listener/*"
      ]
    },
    {
      "Sid" : "Stmt1480452973194",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    },
    {
      "Sid" : "Stmt1480452973195",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeTags"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973196",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973197",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/ES",
            "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}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonPersonalizeFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Personalize melalui AWS Management Console dan SDK. Juga menyediakan akses pilih ke layanan terkait (misalnya, S3, CloudWatch).

`AmazonPersonalizeFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonPersonalizeFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 04 Desember 2018, 22:24 UTC
- Waktu yang telah diedit: 30 Mei 2019, 23:46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonPersonalizeFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "personalize:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::*Personalize*",
        "arn:aws:s3:::*personalize*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "personalize.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonPollyFullAccess

Deskripsi: Memberikan akses penuh ke layanan dan sumber daya Amazon Polly.

`AmazonPollyFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonPollyFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 November 2016, 18:59 UTC
- Waktu telah diedit: 30 November 2016, 18:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPollyFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonPollyReadOnlyAccess

Deskripsi: Memberikan akses hanya-baca ke sumber daya Amazon Polly.

`AmazonPollyReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonPollyReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 November 2016, 18:59 UTC
- Waktu telah diedit: 17 Juli 2018, 16:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPollyReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "polly:DescribeVoices",
        "polly:GetLexicon",
        "polly:GetSpeechSynthesisTask",
        "polly:ListLexicons",
        "polly:ListSpeechSynthesisTasks",
        "polly:SynthesizeSpeech"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonPrometheusConsoleFullAccess

Deskripsi: Memberikan akses penuh ke sumber daya Prometheus AWS Terkelola di konsol AWS

`AmazonPrometheusConsoleFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonPrometheusConsoleFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 15 Desember 2020, 18:11 UTC
- Waktu yang telah diedit: 22 Mei 2025, 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPrometheusConsoleFullAccess`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
        "tag:GetTagValues",
        "tag:GetTagKeys"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aps:CreateWorkspace",
        "aps:DescribeWorkspace",
        "aps:UpdateWorkspaceAlias",
        "aps:DeleteWorkspace",
        "aps:ListWorkspaces",
        "aps:DescribeAlertManagerDefinition",
        "aps:DescribeRuleGroupsNamespace",
        "aps:CreateAlertManagerDefinition",
        "aps:CreateRuleGroupsNamespace",
        "aps:DeleteAlertManagerDefinition",
        "aps:DeleteRuleGroupsNamespace",
        "aps:ListRuleGroupsNamespaces",
        "aps:PutAlertManagerDefinition",
        "aps:PutRuleGroupsNamespace",
        "aps:TagResource",
        "aps:UntagResource",
        "aps:CreateLoggingConfiguration",
        "aps:UpdateLoggingConfiguration",
        "aps:DeleteLoggingConfiguration",
        "aps:DescribeLoggingConfiguration",
        "aps:UpdateWorkspaceConfiguration",
        "aps:DescribeWorkspaceConfiguration",
        "aps:CreateQueryLoggingConfiguration",
        "aps:UpdateQueryLoggingConfiguration",
        "aps:DeleteQueryLoggingConfiguration",
        "aps:DescribeQueryLoggingConfiguration"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonPrometheusFullAccess

Deskripsi: Memberikan akses penuh ke sumber daya Prometheus AWS Terkelola

`AmazonPrometheusFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonPrometheusFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 15 Desember 2020, 18:10 UTC
- Waktu telah diedit: 26 November 2023, 20:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPrometheusFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
        "aps:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeCluster",
      "Effect" : "Allow",
      "Action" : [
        "eks:DescribeCluster",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "aps.amazonaws.com"
          ]
        }
      },
      "Resource" : "*"
    },
    {
      "Sid" : "CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/scraper.aps.amazonaws.com/
AWSServiceRoleForAmazonPrometheusScraper*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "scraper.aps.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonPrometheusQueryAccess

Deskripsi: Memberikan akses untuk menjalankan kueri terhadap sumber daya AWS Prometheus Terkelola

`AmazonPrometheusQueryAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonPrometheusQueryAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 19 Desember 2020, 01:02 UTC
- Waktu yang telah diedit: 19 Desember 2020, 01:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPrometheusQueryAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "aps:GetLabels",
        "aps:GetMetricMetadata",
        "aps:GetSeries",
        "aps:QueryMetrics"
      ],
      "Effect" : "Allow",
```

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonPrometheusRemoteWriteAccess

Deskripsi: Memberikan akses tulis hanya ke ruang kerja Prometheus AWS Terkelola

`AmazonPrometheusRemoteWriteAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonPrometheusRemoteWriteAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 19 Desember 2020, 01:04 UTC
- Waktu yang telah diedit: 19 Desember 2020, 01:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPrometheusRemoteWriteAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonPrometheusScraperServiceRolePolicy

Deskripsi: Menyediakan akses ke AWS Sumber Daya yang dikelola atau digunakan oleh Amazon Managed Service untuk Prometheus Collector

`AmazonPrometheusScraperServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 26 November 2023, 14:19 UTC

- Waktu telah diedit: 26 April 2024, 20:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonPrometheusScraperServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonQDeveloperAccess

Deskripsi: Menyediakan akses pengembang untuk mengaktifkan interaksi dengan Amazon Q

`AmazonQDeveloperAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonQDeveloperAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 09 Juli 2024, 08:35 UTC
- Waktu yang telah diedit: 12 Mei 2025, 20:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonQDeveloperAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonQFullAccess

Deskripsi: Menyediakan akses penuh untuk mengaktifkan interaksi dengan Amazon Q

`AmazonQFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonQFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 November 2023, 16:00 UTC
- Waktu yang telah diedit: 12 Mei 2025, 20:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonQFullAccess`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonQLDBConsoleFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon QLDB melalui file. AWS Management Console

`AmazonQLDBConsoleFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonQLDBConsoleFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 05 September 2019, 18:24 UTC
- Waktu yang telah diedit: 04 November 2022, 17.01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonQLDBConsoleFullAccess`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "qldb:CreateLedger",
        "qldb:UpdateLedger",
        "qldb:UpdateLedgerPermissionsMode",
        "qldb:DeleteLedger",
        "qldb:ListLedgers",
        "qldb:DescribeLedger",
        "qldb:ExportJournalToS3",
        "qldb:ListJournalS3Exports",
        "qldb:ListJournalS3ExportsForLedger",
        "qldb:DescribeJournalS3Export",
        "qldb:CancelJournalKinesisStream",
        "qldb:DescribeJournalKinesisStream",
        "qldb:ListJournalKinesisStreamsForLedger",
        "qldb:StreamJournalToKinesis",
        "qldb:GetBlock",
        "qldb:GetDigest",
        "qldb:GetRevision",
        "qldb:TagResource",
        "qldb:UntagResource",
        "qldb:ListTagsForResource",
        "qldb:SendCommand",
        "qldb:ExecuteStatement",
        "qldb:ShowCatalog",
        "qldb:InsertSampleData",
        "qldb:PartiQLCreateTable",
        "qldb:PartiQLCreateIndex",
        "qldb:PartiQLDropTable",
        "qldb:PartiQLDropIndex",
        "qldb:PartiQLUndropTable",
        "qldb:PartiQLDelete",
        "qldb:PartiQLInsert",
        "qldb:PartiQLUpdate",
        "qldb:PartiQLSelect",
        "qldb:PartiQLHistoryFunction",
        "qldb:PartiQLRedact"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dbqms:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:ListStreams",
        "kinesis:DescribeStream"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "qldb.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonQLDBFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon QLDB melalui API layanan.

`AmazonQLDBFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonQLDBFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 05 September 2019, 18:23 UTC
- Waktu yang telah diedit: 04 November 2022, 17.01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonQLDBFullAccess`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "qldb:CreateLedger",
        "qldb:UpdateLedger",
        "qldb:UpdateLedgerPermissionsMode",
        "qldb:DeleteLedger",
        "qldb:ListLedgers",
        "qldb:DescribeLedger",
        "qldb:ExportJournalToS3",
        "qldb:ListJournalS3Exports",
        "qldb:ListJournalS3ExportsForLedger",
        "qldb:DescribeJournalS3Export",
        "qldb:CancelJournalKinesisStream",
```

```
        "qldb:DescribeJournalKinesisStream",
        "qldb:ListJournalKinesisStreamsForLedger",
        "qldb:StreamJournalToKinesis",
        "qldb:GetDigest",
        "qldb:GetRevision",
        "qldb:GetBlock",
        "qldb:TagResource",
        "qldb:UntagResource",
        "qldb:ListTagsForResource",
        "qldb:SendCommand",
        "qldb:PartiQLCreateTable",
        "qldb:PartiQLCreateIndex",
        "qldb:PartiQLDropTable",
        "qldb:PartiQLDropIndex",
        "qldb:PartiQLUndropTable",
        "qldb:PartiQLDelete",
        "qldb:PartiQLInsert",
        "qldb:PartiQLUpdate",
        "qldb:PartiQLSelect",
        "qldb:PartiQLHistoryFunction",
        "qldb:PartiQLRedact"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "qldb.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonQLDBReadOnly

Deskripsi: Menyediakan akses baca saja ke Amazon QLDB.

`AmazonQLDBReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonQLDBReadOnly` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 05 September 2019, 18:19 UTC
- Waktu yang telah diedit: 02 Juli 2021 02:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonQLDBReadOnly`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "qldb:ListLedgers",
        "qldb:DescribeLedger",
        "qldb:ListJournalS3Exports",
```

```
        "qldb:ListJournalS3ExportsForLedger",
        "qldb:DescribeJournalS3Export",
        "qldb:DescribeJournalKinesisStream",
        "qldb:ListJournalKinesisStreamsForLedger",
        "qldb:GetBlock",
        "qldb:GetDigest",
        "qldb:GetRevision",
        "qldb:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonRDSBetaServiceRolePolicy

Deskripsi: Memungkinkan Amazon RDS mengelola AWS sumber daya atas nama Anda.

`AmazonRDSBetaServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 02 Mei 2018, 19:41 UTC
- Waktu yang telah diedit: 07 Agustus 2024, 00:54 UTC

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

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonRDSCustomInstanceProfileRolePolicy

Deskripsi: Memungkinkan Amazon RDS Custom untuk melakukan berbagai tindakan otomatisasi dan tugas manajemen database melalui profil EC2 instans.

`AmazonRDSCustomInstanceProfileRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRDSCustomInstanceProfileRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Februari 2024, 17:42 UTC
- Waktu telah diedit: 20 Maret 2025, 16:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSCustomInstanceProfileRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ssmAgentPermission1",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ssmAgentPermission2",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetManifest",
        "ssm:PutConfigurePackageResult"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ssmAgentPermission3",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetDocument",
        "ssm:DescribeDocument"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/*"
```

```
    },
    {
      "Sid" : "ssmAgentPermission4",
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:OpenControlChannel"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ssmAgentPermission5",
      "Effect" : "Allow",
      "Action" : [
        "ec2messages:AcknowledgeMessage",
        "ec2messages:DeleteMessage",
        "ec2messages:FailMessage",
        "ec2messages:GetEndpoint",
        "ec2messages:GetMessages",
        "ec2messages:SendReply"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "createEc2SnapshotPermission1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot",
        "ec2:CreateSnapshots"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "createEc2SnapshotPermission2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot",
        "ec2:CreateSnapshots"
      ],
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "createEc2SnapshotPermission3",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshots",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "createTagForEc2SnapshotPermission",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
```

```
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ],
          "ec2:CreateAction" : [
            "CreateSnapshot",
            "CreateSnapshots"
          ]
        }
      }
    },
    {
      "Sid" : "rdsCustomS3ObjectPermission",
      "Effect" : "Allow",
      "Action" : [
        "s3:putObject",
        "s3:getObject",
        "s3:getObjectVersion",
        "s3:AbortMultipartUpload",
        "s3:ListMultipartUploadParts"
      ],
      "Resource" : [
        "arn:aws:s3:::do-not-delete-rds-custom-*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "rdsCustomS3BucketPermission",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucketVersions",
        "s3:ListBucketMultipartUploads"
      ],
      "Resource" : [
        "arn:aws:s3:::do-not-delete-rds-custom-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "readSecretsFromCpPermission",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*",
        "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"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonRDSCustomPreviewServiceRolePolicy

Deskripsi: Kebijakan Peran Layanan Pratinjau Kustom Amazon RDS

`AmazonRDSCustomPreviewServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 08 Oktober 2021 21:44 UTC
- Waktu telah diedit: 25 Maret 2025, 22:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSCustomPreviewServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ecc1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeRegions",
        "ec2:DescribeSnapshots",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVolumes",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeImages",
        "ec2:DescribeVpcs",
        "ec2:RegisterImage",
        "ec2:DeregisterImage",
        "ec2:DescribeTags",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:SearchTransitGatewayMulticastGroups",
        "ec2:GetTransitGatewayMulticastDomainAssociations",
        "ec2:DescribeTransitGatewayMulticastDomains",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : [
```

```
        "*"
      ]
    },
    {
      "Sid" : "ecc2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DisassociateIamInstanceProfile",
        "ec2:AssociateIamInstanceProfile",
        "ec2:ReplaceIamInstanceProfileAssociation",
        "ec2:TerminateInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:RebootInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ecc1scoping",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "ecc1scoping2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:ReleaseAddress"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ecc1scoping3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignPrivateIpAddresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccRunInstances1",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
```

```
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccRunInstances2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*",
        "arn:aws:ec2:*:*:placement-group/*"
      ]
    },
    {
      "Sid" : "eccRunInstances3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*::snapshot/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac",
            "custom-oracle"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "RequireImdsV2",
      "Effect" : "Deny",
      "Action" : "ec2:RunInstances",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringNotEquals" : {
          "ec2:MetadataHttpTokens" : "required"
        },
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccRunInstances3keyPair1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:DeleteKeyPair"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*",
        "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:CopySnapshot",
        "ec2:CreateSnapshots"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
```

```
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccSnapshot3",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshots",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "iam1",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListInstanceProfiles",
        "iam:GetInstanceProfile",
        "iam:GetRole",
        "iam:ListRolePolicies",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "iam2",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
```

```
      "Resource" : "arn:aws:iam::*:role/AWSRDSCustom*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "cloudtrail1",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:GetTrailStatus"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:trail/do-not-delete-rds-custom-*"
    },
    {
      "Sid" : "cw1",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:EnableAlarmActions",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "cw2",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:TagResource"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
```

```
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "cw3",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:*"
    },
    {
      "Sid" : "ssm1",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:aws:ssm:*:*:document/*"
    },
    {
      "Sid" : "ssm2",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ssm3",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetCommandInvocation",
        "ssm:GetConnectionStatus",
        "ssm:DescribeInstanceInformation"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "ssm4",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter",
        "ssm:AddTagsToResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/rds/custom-oracle-rac/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ssm5",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/rds/custom-oracle-rac/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eb1",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:TagResource"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
```

```
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eb2",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:DescribeRule",
        "events:EnableRule",
        "events:ListTargetsByRule",
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:DisableRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eb3",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "events:ManagedBy" : [
            "custom.rds-preview.amazonaws.com"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "eb4",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:EnableRule",
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:DisableRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "events:ManagedBy" : [
            "custom.rds-preview.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "eb5",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*"
    },
    {
      "Sid" : "secretmanager1",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource",
        "secretsmanager:CreateSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*",
        "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"
          ]
        }
      }
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonRDSCustomServiceRolePolicy

Deskripsi: Memungkinkan Amazon RDS Custom untuk mengelola AWS sumber daya atas nama Anda.

`AmazonRDSCustomServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 08 Oktober 2021 21:39 UTC
- Waktu telah diedit: 25 Maret 2025, 23:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSCustomServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v12 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "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:CopySnapshot",
        "ec2:CreateSnapshot",
        "ec2:CreateSnapshots"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccSnapshot3",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshots",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "eccSnapshot4",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshot",
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-sqlserver"
          ]
        }
      }
    },
    {
      "Sid" : "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" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonRDSDataFullAccess

Deskripsi: Memungkinkan akses penuh untuk menggunakan data RDS APIs, penyimpanan rahasia APIs untuk kredensil basis data RDS, dan manajemen kueri konsol DB APIs untuk mengeksekusi pernyataan SQL pada klaster Aurora Tanpa Server di. Akun AWS

`AmazonRDSDataFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRDSDataFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 20 November 2018, 21:29 UTC
- Waktu diedit: 20 November 2019, 21:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSDataFullAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecretsManagerDbCredentialsAccess",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutResourcePolicy",
        "secretsmanager:PutSecretValue",
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:rds-db-credentials/*"
    },
    {
      "Sid" : "RDSDataServiceAccess",
      "Effect" : "Allow",
      "Action" : [
        "dbqms:CreateFavoriteQuery",
        "dbqms:DescribeFavoriteQueries",
        "dbqms:UpdateFavoriteQuery",
        "dbqms:DeleteFavoriteQueries",
        "dbqms:GetQueryString",
        "dbqms:CreateQueryHistory",
        "dbqms:DescribeQueryHistory",
        "dbqms:UpdateQueryHistory",
        "dbqms:DeleteQueryHistory",
        "rds-data:ExecuteSql",
        "rds-data:ExecuteStatement",
        "rds-data:BatchExecuteStatement",
        "rds-data:BeginTransaction",
```

```
        "rds-data:CommitTransaction",
        "rds-data:RollbackTransaction",
        "secretsmanager:CreateSecret",
        "secretsmanager:ListSecrets",
        "secretsmanager:GetRandomPassword",
        "tag:GetResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonRDSDirectoryServiceAccess

Deskripsi: Izinkan RDS mengakses Directory Service Managed AD atas nama pelanggan untuk instans SQL Server DB yang bergabung dengan domain.

`AmazonRDSDirectoryServiceAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRDSDirectoryServiceAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 26 Februari 2016, 02:02 UTC
- Waktu yang telah diedit: 15 Mei 2019, 16:51 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonRDSDirectoryServiceAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ds:DescribeDirectories",
        "ds:AuthorizeApplication",
        "ds:UnauthorizeApplication",
        "ds:GetAuthorizedApplicationDetails"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonRDSEnhancedMonitoringRole

Deskripsi: Menyediakan akses ke Cloudwatch untuk RDS Enhanced Monitoring

`AmazonRDSEnhancedMonitoringRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRDSEnhancedMonitoringRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 11 November 2015, 19:58 UTC
- Waktu telah diedit: 11 November 2015, 19:58 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonRDSEnhancedMonitoringRole`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EnableCreationAndManagementOfRDSCloudwatchLogGroups",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:RDS*"
      ]
    },
    {
      "Sid" : "EnableCreationAndManagementOfRDSCloudwatchLogStreams",
      "Effect" : "Allow",
```

```
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:RDS*:log-stream:*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonRDSFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon RDS melalui. AWS Management Console

`AmazonRDSFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRDSFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu telah diedit: Agustus 17, 2023, 23:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSFullAccess`

Versi kebijakan

Versi kebijakan: v14 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:*",
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricData",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCoipPools",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLocalGatewayRouteTablePermissions",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeLocalGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:GetCoipPoolUsage",
```

```
        "sns:ListSubscriptions",
        "sns:ListTopics",
        "sns:Publish",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "outposts:GetOutpostInstanceTypes",
        "devops-guru:GetResourceCollection"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "pi:*",
      "Resource" : [
        "arn:aws:pi:*:*:metrics/rds/*",
        "arn:aws:pi:*:*:perf-reports/rds/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : [
            "rds.amazonaws.com",
            "rds.application-autoscaling.amazonaws.com"
          ]
        }
      }
    },
    {
      "Action" : [
        "devops-guru:SearchInsights",
        "devops-guru:ListAnomaliesForInsight"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "devops-guru:ServiceNames" : [
            "RDS"
          ]
        },
```

```
        "Null" : {
          "devops-guru:ServiceNames" : "false"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonRDSPerformanceInsightsFullAccess

Deskripsi: Menyediakan akses penuh ke RDS Performance Insights melalui AWS Management Console

`AmazonRDSPerformanceInsightsFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRDSPerformanceInsightsFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 15 Agustus 2023, 23:41 UTC
- Waktu yang telah diedit: 23 Oktober 2023, 21:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSPerformanceInsightsFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRDSPerformanceInsightsReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "pi:DescribeDimensionKeys",
        "pi:GetDimensionKeyDetails",
        "pi:GetResourceMetadata",
        "pi:GetResourceMetrics",
        "pi:ListAvailableResourceDimensions",
        "pi:ListAvailableResourceMetrics"
      ],
      "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsAnalisysReportFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "pi:CreatePerformanceAnalysisReport",
        "pi:GetPerformanceAnalysisReport",
        "pi:ListPerformanceAnalysisReports",
        "pi:DeletePerformanceAnalysisReport"
      ],
      "Resource" : "arn:aws:pi:*:*:perf-reports/rds/*/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsTaggingFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "pi:TagResource",
        "pi:UntagResource",
        "pi:ListTagsForResource"
      ],
      "Resource" : "arn:aws:pi:*:*:*/rds/*"
    },
```

```
    {
      "Sid" : "AmazonRDSDescribeInstanceAccess",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonCloudWatchReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonRDSPerformanceInsightsReadOnly

Deskripsi: Kebijakan Read-Only untuk RDS Performance Insights

`AmazonRDSPerformanceInsightsReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRDSPerformanceInsightsReadOnly` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 05 April 2022, 00:02 UTC
- Waktu yang telah diedit: 23 Oktober 2023, 21:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSPerformanceInsightsReadOnly`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRDSDescribeDBInstances",
      "Effect" : "Allow",
      "Action" : "rds:DescribeDBInstances",
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonRDSDescribeDBClusters",
      "Effect" : "Allow",
      "Action" : "rds:DescribeDBClusters",
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsDescribeDimensionKeys",
      "Effect" : "Allow",
      "Action" : "pi:DescribeDimensionKeys",
      "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsGetDimensionKeyDetails",
```

```
      "Effect" : "Allow",
      "Action" : "pi:GetDimensionKeyDetails",
      "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsGetResourceMetadata",
      "Effect" : "Allow",
      "Action" : "pi:GetResourceMetadata",
      "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsGetResourceMetrics",
      "Effect" : "Allow",
      "Action" : "pi:GetResourceMetrics",
      "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsListAvailableResourceDimensions",
      "Effect" : "Allow",
      "Action" : "pi:ListAvailableResourceDimensions",
      "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsListAvailableResourceMetrics",
      "Effect" : "Allow",
      "Action" : "pi:ListAvailableResourceMetrics",
      "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsGetPerformanceAnalysisReport",
      "Effect" : "Allow",
      "Action" : "pi:GetPerformanceAnalysisReport",
      "Resource" : "arn:aws:pi:*:*:perf-reports/rds/*/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsListPerformanceAnalysisReports",
      "Effect" : "Allow",
      "Action" : "pi:ListPerformanceAnalysisReports",
      "Resource" : "arn:aws:pi:*:*:perf-reports/rds/*/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsListTagsForResource",
      "Effect" : "Allow",
      "Action" : "pi:ListTagsForResource",
```

```
      "Resource" : "arn:aws:pi:*:*:*/rds/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonRDSPreviewServiceRolePolicy

Deskripsi: Kebijakan Peran Layanan Pratinjau Amazon RDS

`AmazonRDSPreviewServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 31 Mei 2018, 18:02 UTC
- Waktu telah diedit: 07 Agustus 2024, 01:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSPreviewServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:CrossRegionCommunication"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AssociateAddress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateCoipPoolPermission",
        "ec2:CreateLocalGatewayRouteTablePermission",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteCoipPoolPermission",
        "ec2:DeleteLocalGatewayRouteTablePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCoipPools",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLocalGatewayRouteTablePermissions",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeLocalGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:DisassociateAddress",
```

```
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ReleaseAddress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "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"
        }
      }
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonRDSReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon RDS melalui. AWS Management Console

`AmazonRDSReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRDSReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu telah diedit: 14 April 2023, 12:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:Describe*",
        "rds:ListTagsForResource",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricData",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "devops-guru:GetResourceCollection"
      ],
      "Resource" : "*"
    },
    {
      "Action" : [
        "devops-guru:SearchInsights",
        "devops-guru:ListAnomaliesForInsight"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "devops-guru:ServiceNames" : [
            "RDS"
          ]
        },
        "Null" : {
          "devops-guru:ServiceNames" : "false"
        }
      }
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonRDSServiceRolePolicy

Deskripsi: Memungkinkan Amazon RDS mengelola AWS sumber daya atas nama Anda.

`AmazonRDSServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 08 Januari 2018, 18:17 UTC
- Waktu telah diedit: 01 Juli 2024, 22:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v14 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CrossRegionCommunication",
      "Effect" : "Allow",
      "Action" : [
        "rds:CrossRegionCommunication"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Ec2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AssociateAddress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateCoipPoolPermission",
        "ec2:CreateLocalGatewayRouteTablePermission",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteCoipPoolPermission",
        "ec2:DeleteLocalGatewayRouteTablePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCoipPools",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLocalGatewayRouteTablePermissions",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeLocalGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:DisassociateAddress",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifyVpcEndpoint",
```

```
        "ec2:ReleaseAddress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeVpcEndpoints",
        "ec2:DeleteVpcEndpoints",
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "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"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonRedshiftAllCommandsFullAccess

Deskripsi: Kebijakan ini mencakup izin untuk menjalankan perintah SQL untuk menyalin, memuat, membongkar, membuat kueri, dan menganalisis data di Amazon Redshift. Kebijakan ini juga

memberikan izin untuk menjalankan pernyataan tertentu untuk layanan terkait, seperti Amazon S3, log Amazon, CloudWatch Amazon, atau SageMaker Glue. AWS

`AmazonRedshiftAllCommandsFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRedshiftAllCommandsFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 04 November 2021 00:48 UTC
- Waktu yang telah diedit: 25 November 2021 02:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftAllCommandsFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonRedshiftDataFullAccess

Deskripsi: Kebijakan ini menyediakan akses penuh ke Data Amazon Redshift. APIs Kebijakan ini juga memberikan akses terbatas ke layanan lain yang diperlukan.

`AmazonRedshiftDataFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRedshiftDataFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 09 September 2020, 19:23 UTC
- Waktu yang telah diedit: 07 April 2023, 18:18 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftDataFullAccess`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataAPIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:BatchExecuteStatement",
        "redshift-data:ExecuteStatement",
        "redshift-data:CancelStatement",
        "redshift-data:ListStatements",
        "redshift-data:GetStatementResult",
```

```
        "redshift-data:DescribeStatement",
        "redshift-data:ListDatabases",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables",
        "redshift-data:DescribeTable"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:ResourceTag/RedshiftDataFullAccess" : "*"
        }
      }
    },
    {
      "Sid" : "GetCredentialsForAPIUser",
      "Effect" : "Allow",
      "Action" : "redshift:GetClusterCredentials",
      "Resource" : [
        "arn:aws:redshift:*:*:dbname:*/*",
        "arn:aws:redshift:*:*:dbuser:*/redshift_data_api_user"
      ]
    },
    {
      "Sid" : "GetCredentialsWithFederatedIAMCredentials",
      "Effect" : "Allow",
      "Action" : "redshift:GetClusterCredentialsWithIAM",
      "Resource" : "arn:aws:redshift:*:*:dbname:*/*"
    },
    {
      "Sid" : "GetCredentialsForServerless",
      "Effect" : "Allow",
      "Action" : "redshift-serverless:GetCredentials",
      "Resource" : "arn:aws:redshift-serverless:*:*:workgroup/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/RedshiftDataFullAccess" : "*"
```

```
        }
      }
    },
    {
      "Sid" : "DenyCreateAPIUser",
      "Effect" : "Deny",
      "Action" : "redshift:CreateClusterUser",
      "Resource" : [
        "arn:aws:redshift:*:*:dbuser:*/redshift_data_api_user"
      ]
    },
    {
      "Sid" : "ServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/redshift-data.amazonaws.com/
AWSServiceRoleForRedshift",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "redshift-data.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonRedshiftFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Redshift melalui file. AWS Management Console

`AmazonRedshiftFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRedshiftFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu yang telah diedit: 07 Juli 2022, 23.31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftFullAccess`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "redshift:*",
        "redshift-serverless:*",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeInternetGateways",
        "sns:CreateTopic",
        "sns:Get*",
        "sns:List*",
        "cloudwatch:Describe*",
        "cloudwatch:Get*",
```

```
        "cloudwatch:List*",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:EnableAlarmActions",
        "cloudwatch:DisableAlarmActions",
        "tag:GetResources",
        "tag:UntagResources",
        "tag:GetTagValues",
        "tag:GetTagKeys",
        "tag:TagResources"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/redshift.amazonaws.com/
AWSServiceRoleForRedshift",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "redshift.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DataAPIPermissions",
      "Action" : [
        "redshift-data:ExecuteStatement",
        "redshift-data:CancelStatement",
        "redshift-data:ListStatements",
        "redshift-data:GetStatementResult",
        "redshift-data:DescribeStatement",
        "redshift-data:ListDatabases",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables",
        "redshift-data:DescribeTable"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerListPermissions",
      "Action" : [
        "secretsmanager:ListSecrets"
```

```
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerCreateGetPermissions",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:TagResource"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:ResourceTag/RedshiftDataFullAccess" : "*"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonRedshiftQueryEditor

Deskripsi: Menyediakan akses penuh ke Editor Kueri Amazon Redshift dan ke kueri yang disimpan melalui file. AWS Management Console

`AmazonRedshiftQueryEditor`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRedshiftQueryEditor` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 04 Oktober 2018, 22:50 UTC
- Waktu yang telah diedit: 16 Februari 2021 19:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditor`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "redshift:GetClusterCredentials",
        "redshift:ListSchemas",
        "redshift:ListTables",
        "redshift:ListDatabases",
        "redshift:ExecuteQuery",
        "redshift:FetchResults",
        "redshift:CancelQuery",
        "redshift:DescribeClusters",
        "redshift:DescribeQuery",
        "redshift:DescribeTable",
        "redshift:ViewQueriesFromConsole",
        "redshift:DescribeSavedQueries",
        "redshift:CreateSavedQuery",
        "redshift:DeleteSavedQueries",
        "redshift:ModifySavedQuery"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "DataAPIPermissions",
      "Action" : [
        "redshift-data:ExecuteStatement",
        "redshift-data:ListDatabases",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables",
        "redshift-data:DescribeTable"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "DataAPIIAMSessionPermissionsRestriction",
      "Action" : [
        "redshift-data:GetStatementResult",
        "redshift-data:CancelStatement",
        "redshift-data:DescribeStatement",
        "redshift-data:ListStatements"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "redshift-data:statement-owner-iam-userid" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "SecretsManagerListPermissions",
      "Action" : [
        "secretsmanager:ListSecrets"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerCreateGetPermissions",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:TagResource"
      ],
```

```
      "Effect" : "Allow",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/RedshiftQueryOwner" : "${aws:userid}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonRedshiftQueryEditorV2FullAccess

Deskripsi: Memberikan akses penuh ke operasi dan sumber daya Amazon Redshift Query Editor V2. Kebijakan ini juga memberikan akses ke layanan lain yang diperlukan. Ini termasuk izin untuk mencantumkan kluster Amazon Redshift, kunci baca, dan alias AWS di KMS dan mengelola rahasia Query Editor V2 di Secrets Manager. AWS

`AmazonRedshiftQueryEditorV2FullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRedshiftQueryEditorV2FullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 24 September 2021 14:06 UTC
- Waktu telah diedit: 21 Februari 2024, 17:20 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2FullAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RedshiftPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KeyManagementServicePermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:DeleteSecret",
        "secretsmanager:TagResource"
```

```
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:sqlworkbench!*"
    },
    {
      "Sid" : "ResourceGroupsTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "sqlworkbench.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2Permissions",
      "Effect" : "Allow",
      "Action" : "sqlworkbench:*",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonRedshiftQueryEditorV2NoSharing

Deskripsi: Memberikan kemampuan untuk bekerja dengan Amazon Redshift Query Editor V2 tanpa berbagi sumber daya. Prinsipal yang diberikan hanya dapat membaca, memperbarui, dan menghapus sumber dayanya sendiri tetapi tidak dapat membagikannya. Kebijakan ini juga memberikan akses ke layanan lain yang diperlukan. Ini termasuk izin untuk mencantumkan kluster Amazon Redshift dan mengelola rahasia Query Editor V2 dari prinsipal di Secrets Manager. AWS

`AmazonRedshiftQueryEditorV2NoSharing`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRedshiftQueryEditorV2NoSharing` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 24 September 2021 14:18 UTC
- Waktu telah diedit: 21 Februari 2024, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2NoSharing`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RedshiftPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:DeleteSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:sqlworkbench!*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "ResourceGroupsTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "sqlworkbench.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2NonResourceLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:CreateFolder",
        "sqlworkbench:PutTab",
        "sqlworkbench:BatchDeleteFolder",
        "sqlworkbench:DeleteTab",
        "sqlworkbench:GenerateSession",
        "sqlworkbench:GetAccountInfo",
        "sqlworkbench:GetAccountSettings",
        "sqlworkbench:GetUserInfo",
        "sqlworkbench:GetUserWorkspaceSettings",
        "sqlworkbench:PutUserWorkspaceSettings",
        "sqlworkbench:ListConnections",
        "sqlworkbench:ListFiles",
        "sqlworkbench:ListTabs",
        "sqlworkbench:UpdateFolder",
```

```
        "sqlworkbench:ListRedshiftClusters",
        "sqlworkbench:DriverExecute",
        "sqlworkbench:ListTaggedResources",
        "sqlworkbench:ListQueryExecutionHistory",
        "sqlworkbench:GetQueryExecutionHistory",
        "sqlworkbench:ListNotebooks",
        "sqlworkbench:GetSchemaInference",
        "sqlworkbench:GetAutocompletionMetadata",
        "sqlworkbench:GetAutocompletionResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2CreateOwnedResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:CreateConnection",
        "sqlworkbench:CreateSavedQuery",
        "sqlworkbench:CreateChart",
        "sqlworkbench:CreateNotebook",
        "sqlworkbench:DuplicateNotebook",
        "sqlworkbench:CreateNotebookFromVersion",
        "sqlworkbench:ImportNotebook"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sqlworkbench-resource-owner" : "${aws: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}"
```

```
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonRedshiftQueryEditorV2ReadSharing

Deskripsi: Memberikan kemampuan untuk bekerja dengan Amazon Redshift Query Editor V2 dengan berbagi sumber daya terbatas. Kepala sekolah yang diberikan dapat membaca, menulis, dan berbagi sumber dayanya sendiri. Prinsipal yang diberikan dapat membaca sumber daya yang dibagikan dengan timnya tetapi tidak dapat memperbaruinya. Kebijakan ini juga memberikan akses ke layanan lain yang diperlukan. Ini termasuk izin untuk mencantumkan kluster Amazon Redshift dan mengelola rahasia Query Editor V2 dari prinsipal di Secrets Manager. AWS

`AmazonRedshiftQueryEditorV2ReadSharing`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRedshiftQueryEditorV2ReadSharing` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 24 September 2021 14:22 UTC
- Waktu telah diedit: 21 Februari 2024, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2ReadSharing`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RedshiftPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:DeleteSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:sqlworkbench!*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "ResourceGroupsTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "tag:GetResources"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "sqlworkbench.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2NonResourceLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:CreateFolder",
        "sqlworkbench:PutTab",
        "sqlworkbench:BatchDeleteFolder",
        "sqlworkbench:DeleteTab",
        "sqlworkbench:GenerateSession",
        "sqlworkbench:GetAccountInfo",
        "sqlworkbench:GetAccountSettings",
        "sqlworkbench:GetUserInfo",
        "sqlworkbench:GetUserWorkspaceSettings",
        "sqlworkbench:PutUserWorkspaceSettings",
        "sqlworkbench:ListConnections",
        "sqlworkbench:ListFiles",
        "sqlworkbench:ListTabs",
        "sqlworkbench:UpdateFolder",
        "sqlworkbench:ListRedshiftClusters",
        "sqlworkbench:DriverExecute",
        "sqlworkbench:ListTaggedResources",
        "sqlworkbench:ListQueryExecutionHistory",
        "sqlworkbench:GetQueryExecutionHistory",
        "sqlworkbench:ListNotebooks",
        "sqlworkbench:GetSchemaInference",
        "sqlworkbench:GetAutocompletionMetadata",
        "sqlworkbench:GetAutocompletionResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2CreateOwnedResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:CreateConnection",
```

```
        "sqlworkbench:CreateSavedQuery",
        "sqlworkbench:CreateChart",
        "sqlworkbench:CreateNotebook",
        "sqlworkbench:DuplicateNotebook",
        "sqlworkbench:CreateNotebookFromVersion",
        "sqlworkbench:ImportNotebook"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sqlworkbench-resource-owner" : "${aws: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}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonRedshiftQueryEditorV2ReadWriteSharing

Deskripsi: Memberikan kemampuan untuk bekerja dengan Amazon Redshift Query Editor V2 dengan berbagi sumber daya. Kepala sekolah yang diberikan dapat membaca, menulis, dan berbagi sumber dayanya sendiri. Kepala sekolah yang diberikan dapat membaca dan memperbarui sumber daya yang dibagikan dengan timnya. Kebijakan ini juga memberikan akses ke layanan lain yang diperlukan. Ini termasuk izin untuk mencantumkan kluster Amazon Redshift dan mengelola rahasia Query Editor V2 dari prinsipal di Secrets Manager. AWS

`AmazonRedshiftQueryEditorV2ReadWriteSharing`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRedshiftQueryEditorV2ReadWriteSharing` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 24 September 2021 14:25 UTC
- Waktu telah diedit: 21 Februari 2024, 17:30 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2ReadWriteSharing`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RedshiftPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:DeleteSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:sqlworkbench!*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "ResourceGroupsTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "sqlworkbench.amazonaws.com"
        }
      }
```

```
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2NonResourceLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:CreateFolder",
        "sqlworkbench:PutTab",
        "sqlworkbench:BatchDeleteFolder",
        "sqlworkbench:DeleteTab",
        "sqlworkbench:GenerateSession",
        "sqlworkbench:GetAccountInfo",
        "sqlworkbench:GetAccountSettings",
        "sqlworkbench:GetUserInfo",
        "sqlworkbench:GetUserWorkspaceSettings",
        "sqlworkbench:PutUserWorkspaceSettings",
        "sqlworkbench:ListConnections",
        "sqlworkbench:ListFiles",
        "sqlworkbench:ListTabs",
        "sqlworkbench:UpdateFolder",
        "sqlworkbench:ListRedshiftClusters",
        "sqlworkbench:DriverExecute",
        "sqlworkbench:ListTaggedResources",
        "sqlworkbench:ListQueryExecutionHistory",
        "sqlworkbench:GetQueryExecutionHistory",
        "sqlworkbench:ListNotebooks",
        "sqlworkbench:GetSchemaInference",
        "sqlworkbench:GetAutocompletionMetadata",
        "sqlworkbench:GetAutocompletionResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2CreateOwnedResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:CreateConnection",
        "sqlworkbench:CreateSavedQuery",
        "sqlworkbench:CreateChart",
        "sqlworkbench:CreateNotebook",
        "sqlworkbench:DuplicateNotebook",
        "sqlworkbench:CreateNotebookFromVersion",
        "sqlworkbench:ImportNotebook"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sqlworkbench-resource-owner" : "${aws: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}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonRedshiftReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon Redshift melalui file. AWS Management Console

`AmazonRedshiftReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRedshiftReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu yang telah diedit: 08 Februari 2024, 00:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRedshiftReadOnlyAccess",
      "Action" : [
        "redshift:Describe*",
        "redshift:ListRecommendations",
        "redshift:ViewQueriesInConsole",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeInternetGateways",
        "sns:Get*",
        "sns:List*",
        "cloudwatch:Describe*",
        "cloudwatch:List*",
        "cloudwatch:Get*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonRedshiftServiceLinkedRolePolicy

Deskripsi: Memungkinkan Amazon Redshift untuk memanggil AWS layanan atas nama Anda

`AmazonRedshiftServiceLinkedRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 18 September 2017, 19:19 UTC
- Waktu telah diedit: 19 Februari 2025, 17:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRedshiftServiceLinkedRolePolicy`

Versi kebijakan

Versi kebijakan: v15 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Ec2VpcPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAddresses",
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
```

```
        "ec2:CreateVpcEndpoint",
        "ec2:DeleteVpcEndpoints",
        "ec2:DescribeVpcEndpoints",
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PublicAccessCreateEip",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:elastic-ip/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/Redshift" : "true"
        }
      }
    },
    {
      "Sid" : "PublicAccessReleaseEip",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ReleaseAddress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:elastic-ip/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/Redshift" : "true"
        }
      }
    },
    {
      "Sid" : "EnableCreationAndManagementOfRedshiftCloudwatchLogGroups",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy"
      ],
```

```
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/redshift/*"
      ]
    },
    {
      "Sid" : "EnableCreationAndManagementOfRedshiftCloudwatchLogStreams",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/redshift/*:log-stream:*"
      ]
    },
    {
      "Sid" : "CreateSecurityGroupWithTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/Redshift" : "true"
        }
      }
    },
    {
      "Sid" : "SecurityGroupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:ModifySecurityGroupRules",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/Redshift" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "CreateTagsOnResources",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:internet-gateway/*",
        "arn:aws:ec2:*:*:elastic-ip/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateVpc",
            "CreateSecurityGroup",
            "CreateSubnet",
            "CreateInternetGateway",
            "CreateRouteTable",
            "AllocateAddress"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "VPCPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/Redshift-Serverless",
            "AWS/Redshift"
          ]
        }
      }
    },
    {
      "Sid" : "SecretManager",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:PutSecretValue",
        "secretsmanager:UpdateSecret",
        "secretsmanager:UpdateSecretVersionStage",
        "secretsmanager:RotateSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:redshift!*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "redshift",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SecretsManagerRandomPassword",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetRandomPassword"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IPV6Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignIpv6Addresses",
        "ec2:UnassignIpv6Addresses"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    },
    {
      "Sid" : "ServiceQuotasToCheckCustomerLimits",
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : [
        "arn:aws:servicequotas:*:*:ec2/L-0263D0A3",
        "arn:aws:servicequotas:*:*:vpc/L-29B6F2EB"
      ]
    },
    {
      "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"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonRekognitionCustomLabelsFullAccess

Deskripsi: Kebijakan ini menetapkan izin rekognition dan s3 yang diperlukan oleh fitur Amazon Rekognition Custom Labels.

`AmazonRekognitionCustomLabelsFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRekognitionCustomLabelsFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 08 Januari 2020, 19:18 UTC
- Waktu yang telah diedit: 16 Agustus 2022, 20.20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRekognitionCustomLabelsFullAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetObject",
```

```
        "s3:GetObjectAcl",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::*custom-labels*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "rekognition:CreateProject",
        "rekognition:CreateProjectVersion",
        "rekognition:StartProjectVersion",
        "rekognition:StopProjectVersion",
        "rekognition:DescribeProjects",
        "rekognition:DescribeProjectVersions",
        "rekognition:DetectCustomLabels",
        "rekognition:DeleteProject",
        "rekognition:DeleteProjectVersion",
        "rekognition:TagResource",
        "rekognition:UntagResource",
        "rekognition:ListTagsForResource",
        "rekognition:CreateDataset",
        "rekognition:ListDatasetEntries",
        "rekognition:ListDatasetLabels",
        "rekognition:DescribeDataset",
        "rekognition:UpdateDatasetEntries",
        "rekognition:DistributeDatasetEntries",
        "rekognition:DeleteDataset",
        "rekognition:CopyProjectVersion",
        "rekognition:PutProjectPolicy",
        "rekognition:ListProjectPolicies",
        "rekognition:DeleteProjectPolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonRekognitionFullAccess

Deskripsi: Akses ke semua Amazon Rekognition APIs

`AmazonRekognitionFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRekognitionFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 November 2016, 14:40 UTC
- Waktu telah diedit: 30 November 2016, 14:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRekognitionFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonRekognitionReadOnlyAccess

Deskripsi: Akses ke semua Read rekognition APIs

`AmazonRekognitionReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRekognitionReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 November 2016, 14:58 UTC
- Waktu telah diedit: November 08, 2023, 18:30 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRekognitionReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v10 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRekognitionReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "rekognition:CompareFaces",
        "rekognition:DetectFaces",
        "rekognition:DetectLabels",
        "rekognition:ListCollections",
        "rekognition:ListFaces",
        "rekognition:SearchFaces",
        "rekognition:SearchFacesByImage",
        "rekognition:DetectText",
        "rekognition:GetCelebrityInfo",
        "rekognition:RecognizeCelebrities",
        "rekognition:DetectModerationLabels",
        "rekognition:GetLabelDetection",
        "rekognition:GetFaceDetection",
        "rekognition:GetContentModeration",
        "rekognition:GetPersonTracking",
        "rekognition:GetCelebrityRecognition",
        "rekognition:GetFaceSearch",
        "rekognition:GetTextDetection",
        "rekognition:GetSegmentDetection",
        "rekognition:DescribeStreamProcessor",
        "rekognition:ListStreamProcessors",
        "rekognition:DescribeProjects",
        "rekognition:DescribeProjectVersions",
        "rekognition:DetectCustomLabels",
        "rekognition:DetectProtectiveEquipment",
        "rekognition:ListTagsForResource",
        "rekognition:ListDatasetEntries",
        "rekognition:ListDatasetLabels",
        "rekognition:DescribeDataset",
        "rekognition:ListProjectPolicies",
        "rekognition:ListUsers",
        "rekognition:SearchUsers",
        "rekognition:SearchUsersByImage",
        "rekognition:GetMediaAnalysisJob",
```

```
        "rekognition:ListMediaAnalysisJobs"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonRekognitionServiceRole

Deskripsi: Memungkinkan Rekognition untuk AWS memanggil layanan atas nama Anda.

`AmazonRekognitionServiceRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRekognitionServiceRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 29 November 2017, 16:52 UTC
- Waktu telah diedit: 29 November 2017, 16:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonRekognitionServiceRole`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : "arn:aws:sns:*:*:AmazonRekognition*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:PutRecord",
        "kinesis:PutRecords"
      ],
      "Resource" : "arn:aws:kinesis:*:*:stream/AmazonRekognition*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:GetDataEndpoint",
        "kinesisvideo:GetMedia"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonRoute53AutoNamingFullAccess

Deskripsi: Menyediakan akses penuh ke semua tindakan Penamaan Otomatis Route 53.

`AmazonRoute53AutoNamingFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRoute53AutoNamingFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 Januari 2018, 18:40 UTC
- Waktu telah diedit: 18 Januari 2018, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53AutoNamingFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
        "route53:ListHostedZonesByName",
        "route53:CreateHostedZone",
        "route53:DeleteHostedZone",
        "route53:ChangeResourceRecordSets",
```

```
        "route53:CreateHealthCheck",
        "route53:GetHealthCheck",
        "route53:DeleteHealthCheck",
        "route53:UpdateHealthCheck",
        "ec2:DescribeVpcs",
        "ec2:DescribeRegions",
        "servicediscovery:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonRoute53AutoNamingReadOnlyAccess

Deskripsi: Menyediakan akses hanya-baca ke semua tindakan Penamaan Otomatis Route 53.

`AmazonRoute53AutoNamingReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRoute53AutoNamingReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 Januari 2018, 03:02 UTC
- Waktu telah diedit: 18 Januari 2018, 03:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53AutoNamingReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonRoute53AutoNamingRegistrantAccess

Deskripsi: Menyediakan akses tingkat pendaftar ke tindakan Penamaan Otomatis Route 53.

`AmazonRoute53AutoNamingRegistrantAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRoute53AutoNamingRegistrantAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 12 Maret 2018, 22:33 UTC
- Waktu telah diedit: 12 Maret 2018, 22:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53AutoNamingRegistrantAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
        "route53:ListHostedZonesByName",
        "route53:ChangeResourceRecordSets",
        "route53:CreateHealthCheck",
        "route53:GetHealthCheck",
        "route53:DeleteHealthCheck",
        "route53:UpdateHealthCheck",
        "servicediscovery:Get*",
        "servicediscovery:List*",
        "servicediscovery:RegisterInstance",
        "servicediscovery:DeregisterInstance"
```

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonRoute53DomainsFullAccess

Deskripsi: Menyediakan akses penuh ke semua tindakan Domain Route53 dan Buat Zona yang Dihosting untuk memungkinkan pembuatan Zona Dihosting sebagai bagian dari pendaftaran domain.

`AmazonRoute53DomainsFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRoute53DomainsFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu telah diedit: 06 Februari 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53DomainsFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:CreateHostedZone",
        "route53domains:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonRoute53DomainsReadOnlyAccess

Deskripsi: Menyediakan akses ke daftar dan tindakan Route53 Domain.

`AmazonRoute53DomainsReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRoute53DomainsReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu telah diedit: 06 Februari 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53DomainsReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53domains:Get*",
        "route53domains:List*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonRoute53FullAccess

Deskripsi: Menyediakan akses penuh ke semua Amazon Route 53 melalui AWS Management Console.

`AmazonRoute53FullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRoute53FullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu yang telah diedit: 15 Mei 2025, 18:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53FullAccess`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonRoute53ProfilesFullAccess

Deskripsi: Kebijakan ini memberikan akses penuh ke sumber daya Profil Amazon Route 53.

`AmazonRoute53ProfilesFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRoute53ProfilesFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 April 2024, 18:30 UTC
- Waktu telah diedit: 27 Agustus 2024, 19:18 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ProfilesFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonRoute53ProfilesReadOnlyAccess

Deskripsi: Kebijakan ini memberikan akses hanya-baca ke sumber daya Profil Amazon Route 53.

`AmazonRoute53ProfilesReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRoute53ProfilesReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 April 2024, 18:29 UTC
- Waktu telah diedit: 27 Agustus 2024, 18:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ProfilesReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonRoute53ReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke semua Amazon Route 53 melalui AWS Management Console.

`AmazonRoute53ReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRoute53ReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu telah diedit: 15 November 2016, 21:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:Get*",
        "route53:List*",
        "route53:TestDNSAnswer"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonRoute53RecoveryClusterFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Route 53 Recovery Cluster

`AmazonRoute53RecoveryClusterFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRoute53RecoveryClusterFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 Agustus 2021 18:37 UTC
- Waktu yang telah diedit: 18 Agustus 2021, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryClusterFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-cluster:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonRoute53RecoveryClusterReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon Route 53 Recovery Cluster

`AmazonRoute53RecoveryClusterReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRoute53RecoveryClusterReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 Agustus 2021 17:36 UTC
- Waktu yang telah diedit: 01 April 2022, 17.37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryClusterReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-cluster:GetRoutingControlState",
        "route53-recovery-cluster:ListRoutingControls"
```

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonRoute53RecoveryControlConfigFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Route 53 Recovery Control Config

`AmazonRoute53RecoveryControlConfigFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRoute53RecoveryControlConfigFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 Agustus 2021 17:48 UTC
- Waktu yang telah diedit: Agustus 18, 2021, 17:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryControlConfigFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-control-config:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonRoute53RecoveryControlConfigReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon Route 53 Recovery Control Config

`AmazonRoute53RecoveryControlConfigReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRoute53RecoveryControlConfigReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 Agustus 2021, 18:01 UTC

- Waktu yang telah diedit: 18 Oktober 2023, 17:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryControlConfigReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-control-config:DescribeCluster",
        "route53-recovery-control-config:DescribeControlPanel",
        "route53-recovery-control-config:DescribeRoutingControl",
        "route53-recovery-control-config:DescribeRoutingControlByName",
        "route53-recovery-control-config:DescribeSafetyRule",
        "route53-recovery-control-config:GetResourcePolicy",
        "route53-recovery-control-config:ListAssociatedRoute53HealthChecks",
        "route53-recovery-control-config:ListClusters",
        "route53-recovery-control-config:ListControlPanels",
        "route53-recovery-control-config:ListRoutingControls",
        "route53-recovery-control-config:ListSafetyRules",
        "route53-recovery-control-config:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonRoute53RecoveryReadinessFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Route 53 Recovery Readiness

`AmazonRoute53RecoveryReadinessFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRoute53RecoveryReadinessFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 Agustus 2021 16:45 UTC
- Waktu yang telah diedit: 18 Agustus 2021, 16:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryReadinessFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      "Action" : [
        "route53-recovery-readiness:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonRoute53RecoveryReadinessReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon Route 53 Recovery Readiness

`AmazonRoute53RecoveryReadinessReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRoute53RecoveryReadinessReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 Agustus 2021 18:11 UTC
- Waktu yang telah diedit: 09 November 2021, 20:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryReadinessReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-readiness:GetCell",
        "route53-recovery-readiness:GetReadinessCheck",
        "route53-recovery-readiness:GetReadinessCheckResourceStatus",
        "route53-recovery-readiness:GetReadinessCheckStatus",
        "route53-recovery-readiness:GetRecoveryGroup",
        "route53-recovery-readiness:GetRecoveryGroupReadinessSummary",
        "route53-recovery-readiness:GetResourceSet",
        "route53-recovery-readiness:ListCells",
        "route53-recovery-readiness:ListCrossAccountAuthorizations",
        "route53-recovery-readiness:ListReadinessChecks",
        "route53-recovery-readiness:ListRecoveryGroups",
        "route53-recovery-readiness:ListResourceSets",
        "route53-recovery-readiness:ListRules",
        "route53-recovery-readiness:ListTagsForResources"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-readiness:GetArchitectureRecommendations",
        "route53-recovery-readiness:GetCellReadinessSummary"
      ],
      "Resource" : "arn:aws:route53-recovery-readiness::*:*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonRoute53ResolverFullAccess

Deskripsi: Kebijakan akses penuh untuk Route 53 Resolver

`AmazonRoute53ResolverFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRoute53ResolverFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 Mei 2019, 18:10 UTC
- Waktu telah diedit: Agustus 05, 2024, 20:06 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ResolverFullAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
  "Statement" : [
    {
      "Sid" : "AmazonRoute53ResolverFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:*",
        "ec2:DescribeSubnets",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfaces",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonRoute53ResolverReadOnlyAccess

Deskripsi: Kebijakan baca saja untuk Route 53 Resolver

`AmazonRoute53ResolverReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRoute53ResolverReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 Mei 2019, 18:11 UTC
- Waktu telah diedit: Agustus 05, 2024, 18:54 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ResolverReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRoute53ResolverReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:Get*",
        "route53resolver:List*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonS3FullAccess

Deskripsi: Menyediakan akses penuh ke semua ember melalui. AWS Management Console

`AmazonS3FullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonS3FullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu yang telah diedit: 27 September 2021, 20:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3FullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:*",
        "s3-object-lambda:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonS3ObjectLambdaExecutionRolePolicy

Deskripsi: Menyediakan izin fungsi AWS Lambda untuk berinteraksi dengan Amazon S3 Object Lambda. Juga memberikan izin Lambda untuk menulis ke Log. CloudWatch

`AmazonS3ObjectLambdaExecutionRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonS3ObjectLambdaExecutionRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 18 Agustus 2021 10:07 UTC
- Waktu yang telah diedit: Agustus 18, 2021, 10:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonS3ObjectLambdaExecutionRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "s3-object-lambda:WriteGetObjectResponse"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonS3OutpostsFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon S3 di Outposts melalui. AWS Management Console

`AmazonS3OutpostsFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonS3OutpostsFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 02 Oktober 2020, 17:26 UTC
- Waktu yang telah diedit: 02 Oktober 2020, 17:26 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3OutpostsFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "s3-outposts:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "datasync:ListTasks",
        "datasync:ListLocations",
        "datasync:DescribeTask",
        "datasync:DescribeLocation*"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "outposts:ListOutposts",
        "outposts:GetOutpost"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonS3OutpostsReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon S3 di Outposts melalui. AWS Management Console

`AmazonS3OutpostsReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonS3OutpostsReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 02 Oktober 2020, 18:55 UTC
- Waktu yang telah diedit: 02 Oktober 2020, 18:55 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3OutpostsReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3-outposts:Get*",
        "s3-outposts:List*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "datasync:ListTasks",
        "datasync:ListLocations",
        "datasync:DescribeTask",
        "datasync:DescribeLocation*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "outposts:ListOutposts",
        "outposts:GetOutpost"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonS3ReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke semua bucket melalui. AWS Management Console

`AmazonS3ReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonS3ReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu yang telah diedit: 10 Agustus 2023, 21:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:Get*",
        "s3:List*",
        "s3:Describe*",
        "s3-object-lambda:Get*",
        "s3-object-lambda:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonS3TablesFullAccess

Deskripsi: Menyediakan akses penuh ke semua bucket tabel S3.

`AmazonS3TablesFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonS3TablesFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 Desember 2024, 15:21 UTC
- Waktu yang telah diedit: 03 Desember 2024, 15:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3TablesFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3tables:*"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonS3TablesLakeFormationServiceRole

Deskripsi: Kebijakan terkelola ini memberikan izin AWS Lake Formation untuk bertindak pada semua bucket tabel, ruang nama, dan tabel dalam akun.

`AmazonS3TablesLakeFormationServiceRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonS3TablesLakeFormationServiceRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 19 Juni 2025, 19:07 UTC
- Waktu yang telah diedit: 09 Juli 2025, 22:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonS3TablesLakeFormationServiceRole`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "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}"
        }
```

```
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonS3TablesReadOnlyAccess

Deskripsi: Menyediakan akses hanya baca ke semua bucket tabel S3.

`AmazonS3TablesReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonS3TablesReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 Desember 2024, 15:21 UTC
- Waktu telah diedit: 03 Desember 2024, 15:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3TablesReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3tables:Get*",
        "s3tables:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy

Deskripsi: Kebijakan peran layanan yang digunakan oleh layanan Layanan AWS Katalog untuk menyediakan produk dari SageMaker portofolio produk Amazon. Memberikan izin ke serangkaian layanan terkait termasuk CodePipeline,, CodeBuild, CodeCommit Glue, CloudFormation, dll.

`AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 November 2020, 18:48 UTC
- Waktu telah diedit: 01 Juli 2024, 07:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "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/*",
      "Condition" : {
        "StringEquals" : {
          "codestar-connections:PassedToService" : "codepipeline.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCodeConnectionPermission",
      "Effect" : "Allow",
      "Action" : "codeconnections:PassConnection",
      "Resource" : "arn:aws:codeconnections:*:*:connection/*",
      "Condition" : {
        "StringEquals" : {
          "codeconnections:PassedToService" : "codepipeline.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSageMakerCanvasAIServicesAccess

Deskripsi: Memberikan izin bagi Amazon SageMaker Canvas untuk menggunakan layanan AI guna mendukung solusi AI yang siap digunakan. Kebijakan ini akan menambahkan lebih banyak izin bermutasi untuk layanan saat Amazon SageMaker Canvas menambahkan dukungan.

`AmazonSageMakerCanvasAIServicesAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerCanvasAIServicesAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 23 Maret 2023, 22:36 UTC
- Waktu telah diedit: 29 November 2023, 14:47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasAIServicesAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSageMakerCanvasBedrockAccess

Deskripsi: Kebijakan ini memberikan izin untuk menggunakan Amazon Bedrock di SageMaker Canvas dengan menyediakan akses ke layanan hilir seperti S3.

`AmazonSageMakerCanvasBedrockAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerCanvasBedrockAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 02 Februari 2024, 18:37 UTC
- Waktu telah diedit: 02 Februari 2024, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasBedrockAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "S3CanvasAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
      ],
```

```
      "Resource" : [
        "arn:aws:s3:::sagemaker-*/Canvas",
        "arn:aws:s3:::sagemaker-*/Canvas/*"
      ]
    },
    {
      "Sid" : "S3BucketAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSageMakerCanvasDataPrepFullAccess

Deskripsi: Menyediakan akses penuh ke SageMaker sumber daya Amazon dan operasi untuk persiapan data di Canvas. Kebijakan ini juga menyediakan akses tertentu ke layanan terkait (misalnya, S3, IAM, KMS, RDS, Log, Redshift, Athena CloudWatch , Glue,, Secrets Manager). EventBridge Kebijakan ini harus dilampirkan ke peran eksekusi SageMaker Domain/Profil Pengguna Amazon.

`AmazonSageMakerCanvasDataPrepFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerCanvasDataPrepFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Oktober 2023, 22:56 UTC
- Waktu yang telah diedit: 16 Agustus 2024, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasDataPrepFullAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SageMakerListFeatureGroupOperation",
      "Effect" : "Allow",
      "Action" : "sagemaker:ListFeatureGroups",
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerFeatureGroupOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateFeatureGroup",
        "sagemaker:DescribeFeatureGroup"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:feature-group/*"
    },
    {
      "Sid" : "SageMakerProcessingJobOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateProcessingJob",
```

```
        "sagemaker:DescribeProcessingJob",
        "sagemaker:AddTags"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:processing-job/*canvas-data-prep*"
    },
    {
      "Sid" : "SageMakerProcessingJobListOperation",
      "Effect" : "Allow",
      "Action" : "sagemaker:ListProcessingJobs",
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerPipelineOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribePipeline",
        "sagemaker:CreatePipeline",
        "sagemaker:UpdatePipeline",
        "sagemaker:DeletePipeline",
        "sagemaker:StartPipelineExecution",
        "sagemaker:ListPipelineExecutionSteps",
        "sagemaker:DescribePipelineExecution"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:pipeline/*canvas-data-prep*"
    },
    {
      "Sid" : "KMSListOperations",
      "Effect" : "Allow",
      "Action" : "kms:ListAliases",
      "Resource" : "*"
    },
    {
      "Sid" : "KMSOperations",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
      "Sid" : "S3Operations",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
```

```
        "s3:GetBucketCors",
        "s3:GetBucketLocation",
        "s3:AbortMultipartUpload"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3GetObjectOperation",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/SageMaker" : "true"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3ListOperations",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMListOperations",
      "Effect" : "Allow",
      "Action" : "iam:ListRoles",
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "IAMGetOperations",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Sid" : "IAMPassOperation",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com",
            "events.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "EventBridgePutOperation",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-data-prep-job" : "true"
        }
      }
    },
    {
      "Sid" : "EventBridgeOperations",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:PutTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sagemaker:is-canvas-data-prep-job" : "true"
```

```
        }
      }
    },
    {
      "Sid" : "EventBridgeTagBasedOperations",
      "Effect" : "Allow",
      "Action" : [
        "events:TagResource"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-data-prep-job" : "true",
          "aws:ResourceTag/sagemaker:is-canvas-data-prep-job" : "true"
        }
      }
    },
    {
      "Sid" : "EventBridgeListTagOperation",
      "Effect" : "Allow",
      "Action" : "events:ListTagsForResource",
      "Resource" : "*"
    },
    {
      "Sid" : "GlueOperations",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:SearchTables"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*"
      ]
    },
    {
      "Sid" : "EMROperations",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:ListInstanceGroups"
```

```
      ],
      "Resource" : "arn:aws:elasticmapreduce:*:*:cluster/*"
    },
    {
      "Sid" : "EMRListOperation",
      "Effect" : "Allow",
      "Action" : "elasticmapreduce:ListClusters",
      "Resource" : "*"
    },
    {
      "Sid" : "AthenaListDataCatalogOperation",
      "Effect" : "Allow",
      "Action" : "athena:ListDataCatalogs",
      "Resource" : "*"
    },
    {
      "Sid" : "AthenaQueryExecutionOperations",
      "Effect" : "Allow",
      "Action" : [
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:StartQueryExecution",
        "athena:StopQueryExecution"
      ],
      "Resource" : "arn:aws:athena:*:*:workgroup/*"
    },
    {
      "Sid" : "AthenaDataCatalogOperations",
      "Effect" : "Allow",
      "Action" : [
        "athena:ListDatabases",
        "athena:ListTableMetadata"
      ],
      "Resource" : "arn:aws:athena:*:*:datacatalog/*"
    },
    {
      "Sid" : "RedshiftOperations",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:DescribeStatement",
        "redshift-data:CancelStatement",
        "redshift-data:GetStatementResult"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "RedshiftArnBasedOperations",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:ExecuteStatement",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables"
      ],
      "Resource" : "arn:aws:redshift:*:*:cluster:*"
    },
    {
      "Sid" : "RedshiftGetCredentialsOperation",
      "Effect" : "Allow",
      "Action" : "redshift:GetClusterCredentials",
      "Resource" : [
        "arn:aws:redshift:*:*:dbuser:*/sagemaker_access*",
        "arn:aws:redshift:*:*:dbname:*"
      ]
    },
    {
      "Sid" : "SecretsManagerARNBasedOperation",
      "Effect" : "Allow",
      "Action" : "secretsmanager:CreateSecret",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonSageMaker-*"
    },
    {
      "Sid" : "SecretManagerTagBasedOperation",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonSageMaker-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SageMaker" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RDSOperation",
      "Effect" : "Allow",
```

```
      "Action" : "rds:DescribeDBInstances",
      "Resource" : "*"
    },
    {
      "Sid" : "LoggingOperation",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/sagemaker/studio:*"
    },
    {
      "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}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSageMakerCanvasDirectDeployAccess

Deskripsi: Memungkinkan Amazon SageMaker Canvas membuat, mengelola, dan melihat detail titik akhir untuk titik akhir yang dibuat melalui Canvas. Memungkinkan Amazon SageMaker Canvas untuk mengambil metrik pemanggilan titik akhir dari. CloudWatch

`AmazonSageMakerCanvasDirectDeployAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerCanvasDirectDeployAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 06 Oktober 2023, 18:11 UTC
- Waktu telah diedit: 06 Oktober 2023, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerCanvasDirectDeployAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
        "sagemaker:CreateEndpointConfig",
        "sagemaker:DeleteEndpoint",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:InvokeEndpoint",
        "sagemaker:UpdateEndpoint"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:Canvas*",
        "arn:aws:sagemaker:*:*:canvas*"
      ]
    },
    {
      "Sid" : "ReadCWInvocationMetrics",
      "Effect" : "Allow",
      "Action" : "cloudwatch:GetMetricData",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSageMakerCanvasEMRServerlessExecutionRolePolicy

Deskripsi: Kebijakan ini memberikan izin ke Amazon EMR Tanpa Server untuk layanan seperti S3, yang digunakan oleh Amazon Canvas untuk pemrosesan data besar. SageMaker

`AmazonSageMakerCanvasEMRServerlessExecutionRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerCanvasEMRServerlessExecutionRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Juli 2024, 00:35 UTC
- Waktu yang telah diedit: 27 Juli 2024, 00:35 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasEMRServerlessExecutionRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSageMakerCanvasForecastAccess

Deskripsi: Kebijakan ini memberikan izin yang biasanya diperlukan untuk menggunakan SageMaker Canvas dengan Amazon Forecast.

`AmazonSageMakerCanvasForecastAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerCanvasForecastAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 24 Agustus 2022, 20.04 UTC
- Waktu yang telah diedit: 24 Agustus 2022, 20.04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerCanvasForecastAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-*/Canvas*",
        "arn:aws:s3:::sagemaker-*/canvas*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSageMakerCanvasFullAccess

Deskripsi: Menyediakan akses penuh ke sumber daya dan operasi Amazon SageMaker Canvas. Kebijakan ini juga menyediakan akses tertentu ke layanan terkait (misalnya, S3, IAM, VPC, ECR, Logs, Redshift, Secrets Manager CloudWatch , dan Forecast). Kebijakan ini harus dilampirkan ke peran eksekusi SageMaker Domain/Profil Pengguna Amazon.

`AmazonSageMakerCanvasFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerCanvasFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 09 September 2022, 00:44 UTC
- Waktu telah diedit: 16 Agustus 2024, 04:35 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasFullAccess`

Versi kebijakan

Versi kebijakan: v11 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SageMakerUserDetailsAndPackageOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeUserProfile",
        "sagemaker:ListTags",
        "sagemaker:ListModelPackages",
        "sagemaker:ListModelPackageGroups",
        "sagemaker:ListEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerPackageGroupOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateModelPackageGroup",
        "sagemaker:CreateModelPackage",
        "sagemaker:DescribeModelPackageGroup",
```

```
        "sagemaker:DescribeModelPackage"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:model-package/*",
        "arn:aws:sagemaker:*:*:model-package-group/*"
      ]
    },
    {
      "Sid" : "SageMakerTrainingOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateCompilationJob",
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateModel",
        "sagemaker:CreateProcessingJob",
        "sagemaker:CreateAutoMLJob",
        "sagemaker:CreateAutoMLJobV2",
        "sagemaker: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}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSageMakerCanvasSMDataScienceAssistantAccess

Deskripsi: Menyediakan izin untuk Amazon SageMaker Canvas untuk menggunakan layanan SageMaker Data Science Assistant. Data Science Assistant saat ini menggunakan Amazon SageMaker dan Amazon Q Developer untuk memproses permintaan pengguna.

`AmazonSageMakerCanvasSMDataScienceAssistantAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerCanvasSMDataScienceAssistantAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 04 Desember 2024, 14:06 UTC
- Waktu telah diedit: 13 Januari 2025, 22:52 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasSMDataScienceAssistantAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSageMakerClusterInstanceRolePolicy

Deskripsi: Kebijakan ini memberikan izin yang biasanya diperlukan untuk menggunakan Amazon SageMaker Cluster.

`AmazonSageMakerClusterInstanceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerClusterInstanceRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 November 2023, 15:11 UTC

- Waktu telah diedit: 29 November 2023, 15:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerClusterInstanceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudwatchLogStreamPublishPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/sagemaker/Clusters/*:log-stream:*"
      ]
    },
    {
      "Sid" : "CloudwatchLogGroupCreationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/sagemaker/Clusters/*"
      ]
    },
    {
      "Sid" : "CloudwatchPutMetricDataAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "cloudwatch:PutMetricData"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "/aws/sagemaker/Clusters"
        }
      }
    },
    {
      "Sid" : "DataRetrievalFromS3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SSMConnectivityPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSageMakerCoreServiceRolePolicy

Deskripsi: Kebijakan terkelola untuk Peran Tertaut Layanan untuk Amazon SageMaker Core Services

`AmazonSageMakerCoreServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 21 Desember 2020 21:40 UTC
- Waktu yang telah diedit: 21 Desember 2020, 21:40 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSageMakerCoreServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterfacePermission"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:AuthorizedService" : "sagemaker.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSageMakerEdgeDeviceFleetPolicy

Deskripsi: Menyediakan izin yang diperlukan untuk SageMaker Edge untuk membuat dan mengelola armada perangkat untuk pelanggan menggunakan koneksi cloud default.

`AmazonSageMakerEdgeDeviceFleetPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerEdgeDeviceFleetPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 08 Desember 2020, 16:17 UTC
- Waktu yang telah diedit: 08 Desember 2020, 16:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerEdgeDeviceFleetPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
    {
      "Sid" : "DeviceS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetBucketLocation"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
      ]
    },
    {
      "Sid" : "SageMakerEdgeApis",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:SendHeartbeat",
        "sagemaker:GetDeviceRegistration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateIoTRoleAlias",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateRoleAlias",
        "iot:DescribeRoleAlias",
        "iot:UpdateRoleAlias",
        "iot:ListTagsForResource",
        "iot:TagResource"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:rolealias/SageMakerEdge*"
      ]
    },
    {
      "Sid" : "CreateIoTRoleAliasIamPermissionsGetRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/*SageMaker*",
```

```
        "arn:aws:iam::*:role/*Sagemaker*",
        "arn:aws:iam::*:role/*sagemaker*"
      ]
    },
    {
      "Sid" : "CreateIoTRoleAliasIamPermissionsPassRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/*SageMaker*",
        "arn:aws:iam::*:role/*Sagemaker*",
        "arn:aws:iam::*:role/*sagemaker*"
      ],
      "Condition" : {
        "StringEqualsIfExists" : {
          "iam:PassedToService" : [
            "iot.amazonaws.com",
            "credentials.iot.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSageMakerFeatureStoreAccess

Deskripsi: Memberikan izin yang diperlukan untuk mengaktifkan toko offline untuk grup SageMaker FeatureStore fitur Amazon.

`AmazonSageMakerFeatureStoreAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerFeatureStoreAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Desember 2020, 16:24 UTC
- Waktu telah diedit: 05 Desember 2022, 14.19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerFeatureStoreAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetBucketAcl",
        "s3:PutObjectAcl"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*/metadata/*",
        "arn:aws:s3:::*Sagemaker*/metadata/*",
        "arn:aws:s3:::*sagemaker*/metadata/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:GetTable",
        "glue:UpdateTable"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/sagemaker_featurestore",
        "arn:aws:glue:*:*:table/sagemaker_featurestore/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSageMakerFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon SageMaker melalui AWS Management Console dan SDK. Juga menyediakan akses pilih ke layanan terkait (misalnya, S3, ECR, CloudWatch Log).

`AmazonSageMakerFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 November 2017, 13:07 UTC
- Waktu telah diedit: 04 Desember 2024, 13:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerFullAccess`

Versi kebijakan

Versi kebijakan: v27 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowAllNonAdminSageMakerActions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:*",
        "sagemaker-geospatial:*"
      ],
      "NotResource" : [
        "arn:aws:sagemaker:*:*:domain/*",
        "arn:aws:sagemaker:*:*:user-profile/*",
        "arn:aws:sagemaker:*:*:app/*",
        "arn:aws:sagemaker:*:*:space/*",
        "arn:aws:sagemaker:*:*: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" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSageMakerGeospatialExecutionRole

Deskripsi: Kebijakan ini menyediakan akses ke layanan yang umumnya dibutuhkan untuk menggunakan SageMaker geospasial.

`AmazonSageMakerGeospatialExecutionRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerGeospatialExecutionRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 30 November 2022, 10:08 UTC
- Waktu yang telah diedit: 10 Mei 2023, 20:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerGeospatialExecutionRole`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:PutObject",
```

```
        "s3:GetObject",
        "s3:ListBucketMultipartUploads"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "sagemaker-geospatial:GetEarthObservationJob",
      "Resource" : "arn:aws:sagemaker-geospatial:*:*:earth-observation-job/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "sagemaker-geospatial:GetRasterDataCollection",
      "Resource" : "arn:aws:sagemaker-geospatial:*:*:raster-data-collection/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSageMakerGeospatialFullAccess

Deskripsi: Kebijakan ini memberikan izin yang memungkinkan akses penuh ke Amazon SageMaker Geospasial melalui dan SDK AWS Management Console .

`AmazonSageMakerGeospatialFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerGeospatialFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 30 November 2022, 10:06 UTC
- Waktu yang telah diedit: 30 November 2022, 10.06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerGeospatialFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "sagemaker-geospatial:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker-geospatial.amazonaws.com"
          ]
        }
      }
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSageMakerGroundTruthExecution

Deskripsi: Menyediakan akses ke AWS layanan yang diperlukan untuk menjalankan SageMaker GroundTruth pekerjaan Pelabelan

`AmazonSageMakerGroundTruthExecution`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerGroundTruthExecution` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 09 Juli 2020, 19:30 UTC
- Waktu yang telah diedit: 29 April 2022 20.49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerGroundTruthExecution`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CustomLabelingJobs",
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*GtRecipe*",
        "arn:aws:lambda:*:*:function:*LabelingFunction*",
        "arn:aws:lambda:*:*:function:*SageMaker*",
        "arn:aws:lambda:*:*:function:*sagemaker*",
        "arn:aws:lambda:*:*:function:*Sagemaker*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*GroundTruth*",
        "arn:aws:s3:::*Groundtruth*",
        "arn:aws:s3:::*groundtruth*",
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
```

```
          "s3:ExistingObjectTag/SageMaker" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData",
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "StreamingQueue",
      "Effect" : "Allow",
      "Action" : [
        "sqs:CreateQueue",
        "sqs:DeleteMessage",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ReceiveMessage",
        "sqs:SendMessage",
        "sqs:SetQueueAttributes"
      ],
      "Resource" : "arn:aws:sqs:*:*:*GroundTruth*"
    },
    {
      "Sid" : "StreamingTopicSubscribe",
      "Effect" : "Allow",
      "Action" : "sns:Subscribe",
      "Resource" : [
        "arn:aws:sns:*:*:*GroundTruth*",
```

```
        "arn:aws:sns:*:*:*Groundtruth*",
        "arn:aws:sns:*:*:*groundTruth*",
        "arn:aws:sns:*:*:*groundtruth*",
        "arn:aws:sns:*:*:*SageMaker*",
        "arn:aws:sns:*:*:*Sagemaker*",
        "arn:aws:sns:*:*:*sageMaker*",
        "arn:aws:sns:*:*:*sagemaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "sns:Protocol" : "sqs"
        },
        "StringLike" : {
          "sns:Endpoint" : "arn:aws:sqs:*:*:*GroundTruth*"
        }
      }
    },
    {
      "Sid" : "StreamingTopic",
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:*GroundTruth*",
        "arn:aws:sns:*:*:*Groundtruth*",
        "arn:aws:sns:*:*:*groundTruth*",
        "arn:aws:sns:*:*:*groundtruth*",
        "arn:aws:sns:*:*:*SageMaker*",
        "arn:aws:sns:*:*:*Sagemaker*",
        "arn:aws:sns:*:*:*sageMaker*",
        "arn:aws:sns:*:*:*sagemaker*"
      ]
    },
    {
      "Sid" : "StreamingTopicUnsubscribe",
      "Effect" : "Allow",
      "Action" : [
        "sns:Unsubscribe"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "WorkforceVPC",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeVpcEndpoints",
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "ec2:VpceServiceName" : [
            "*sagemaker-task-resources*",
            "aws.sagemaker*labeling*"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSageMakerHyperPodObservabilityAdminAccess

Deskripsi: Kebijakan ini memberikan hak administratif yang diperlukan untuk menyiapkan SageMaker HyperPod observabilitas. Ini memungkinkan akses ke Amazon Managed Prometheus, Amazon Managed Grafana dan EKS Addons. Kebijakan ini juga mencakup akses luas ke Grafana HTTP APIs melalui ServiceAccountTokens seluruh ruang kerja Grafana yang Dikelola Amazon di akun Anda.

`AmazonSageMakerHyperPodObservabilityAdminAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerHyperPodObservabilityAdminAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 10 Juli 2025, 14:37 UTC
- Waktu yang telah diedit: 10 Juli 2025, 14:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerHyperPodObservabilityAdminAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "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/
AmazonSageMakerHyperPodObservabilityGrafanaAccess-*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "grafana.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "IAMEKSPassRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
```

```
      "Resource" : "arn:aws:iam::*:role/
AmazonSageMakerHyperPodObservabilityAddonAccess-*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "pods.eks.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "IAMGetRoleAccess",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : [
        "arn:aws:iam::*: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" : "EKSAddonDescribePodIdentityAccess",
      "Effect" : "Allow",
      "Action" : "eks:DescribePodIdentityAssociation",
      "Resource" : "arn:aws:eks:*:*:podidentityassociation/*/*"
    },
    {
      "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" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSageMakerHyperPodServiceRolePolicy

Deskripsi: Kebijakan ini memberikan izin ke Amazon SageMaker HyperPod ke AWS layanan terkait seperti Amazon EKS, Amazon, dll. CloudWatch

`AmazonSageMakerHyperPodServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 06 September 2024, 17:04 UTC
- Waktu yang telah diedit: September 06, 2024, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSageMakerHyperPodServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSageMakerMechanicalTurkAccess

Deskripsi: Menyediakan akses untuk membuat sumber daya Amazon Augmented FlowDefinition AI terhadap Tim Kerja mana pun.

`AmazonSageMakerMechanicalTurkAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerMechanicalTurkAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 Desember 2019, 16:19 UTC
- Waktu diedit: 03 Desember 2019, 16:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerMechanicalTurkAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSageMakerModelGovernanceUseAccess

Deskripsi: Kebijakan AWS terkelola ini memberikan izin yang diperlukan untuk menggunakan semua fitur SageMaker Tata Kelola Amazon. Kebijakan ini juga menyediakan akses terpilih ke layanan terkait (misalnya, S3, KMS).

`AmazonSageMakerModelGovernanceUseAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerModelGovernanceUseAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 November 2022, 08:58 UTC
- Waktu yang telah diedit: 04 Juni 2024, 21:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerModelGovernanceUseAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSageMakerModelRegistryFullAccess

Deskripsi: Ini adalah kebijakan terkelola baru untuk Model Registry di Sagemaker. Kebijakan ini adalah kebijakan mandiri yang dapat dilampirkan ke peran pengguna untuk mengakses fungsionalitas terkait Model Registry di Sagemaker.

`AmazonSageMakerModelRegistryFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerModelRegistryFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 13 April 2023, 05:20 UTC
- Waktu yang telah diedit: 06 Juni 2024, 18:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerModelRegistryFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "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"
        }
      }
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSageMakerNotebooksServiceRolePolicy

Deskripsi: Kebijakan terkelola untuk Peran Tertaut Layanan untuk SageMaker Notebook Amazon

`AmazonSageMakerNotebooksServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 18 Oktober 2019 20:27 UTC
- Waktu telah diedit: 14 November 2024, 20:33 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSageMakerNotebooksServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v10 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSageMakerPartnerAppsFullAccess

Deskripsi: Memungkinkan pengguna aplikasi SageMaker mitra Amazon untuk mengakses aplikasi, daftar aplikasi yang tersedia, meluncurkan web aplikasi UIs, dan terhubung melalui SDK aplikasi.

`AmazonSageMakerPartnerAppsFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerPartnerAppsFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 17 Januari 2025, 18:37 UTC
- Waktu telah diedit: 17 Januari 2025, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerPartnerAppsFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceR

Deskripsi: Kebijakan peran layanan yang digunakan oleh AWS APIGateway dalam produk yang AWS ServiceCatalog disediakan dari SageMaker portofolio produk Amazon. Memberikan izin ke serangkaian layanan terkait termasuk Lambda dan lainnya.

`AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 01 Agustus 2023, 15:06 UTC
- Waktu yang telah diedit: Agustus 01, 2023, 15:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "lambda:InvokeFunction",
      "Resource" : "arn:aws:lambda:*:*:function:sagemaker-*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:project-name" : "false",
          "aws:ResourceTag/sagemaker:partner" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "sagemaker:InvokeEndpoint",
      "Resource" : "arn:aws:sagemaker:*:*:endpoint/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:project-name" : "false",
          "aws:ResourceTag/sagemaker:partner" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServ

Deskripsi: Kebijakan peran layanan yang digunakan oleh AWS CloudFormation dalam produk yang AWS ServiceCatalog disediakan dari SageMaker portofolio produk Amazon. Memberikan izin untuk subset layanan terkait termasuk Lambda, dan lainnya. APIGateway

`AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 01 Agustus 2023, 15:06 UTC
- Waktu yang telah diedit: Agustus 01, 2023, 15:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsLambdaRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsApiGatewayRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "apigateway.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:DeleteFunction",
        "lambda:UpdateFunctionCode",
        "lambda:ListTags",
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:sagemaker-*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:project-name" : "false",
```

```
          "aws:ResourceTag/sagemaker:partner" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:TagResource"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:sagemaker-*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:project-name" : "false",
          "aws:ResourceTag/sagemaker:partner" : "false"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "sagemaker:project-name",
            "sagemaker:partner"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:PublishLayerVersion",
        "lambda:GetLayerVersion",
        "lambda:DeleteLayerVersion",
        "lambda:GetFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:layer:sagemaker-*",
        "arn:aws:lambda:*:*:function:sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET",
        "apigateway:DELETE",
```

```
        "apigateway:PATCH",
        "apigateway:POST",
        "apigateway:PUT"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/restapis"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:project-name" : "false",
          "aws:ResourceTag/sagemaker:partner" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:POST",
        "apigateway:PUT"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/tags/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:project-name" : "false",
          "aws:ResourceTag/sagemaker:partner" : "false"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "sagemaker:project-name",
            "sagemaker:partner"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
```

```
        "arn:aws:s3:::sagemaker-*/lambda-auth-code/layer.zip"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRole

Deskripsi: Kebijakan peran layanan yang digunakan oleh AWS Lambda dalam produk yang AWS ServiceCatalog disediakan dari portofolio produk Amazon SageMaker . Memberikan izin ke serangkaian layanan terkait termasuk Secrets Manager dan lainnya.

`AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 01 Agustus 2023, 15:05 UTC

- Waktu yang telah diedit: Agustus 01, 2023, 15:05 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "secretsmanager:GetSecretValue",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:partner" : false
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSageMakerPipelinesIntegrations

Deskripsi: Kebijakan Terkelola Amazon ini memberikan izin yang biasanya diperlukan untuk digunakan dengan langkah Callback dan langkah Lambda di Model Building Pipelines. SageMaker Hal ini ditambahkan ke AmazonSageMaker - ExecutionRole yang dapat dibuat saat mengatur SageMaker Studio. Ini juga dapat dilampirkan ke peran lain yang akan digunakan untuk membuat atau mengeksekusi saluran pipa.

`AmazonSageMakerPipelinesIntegrations`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerPipelinesIntegrations` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 Juli 2021 16:35 UTC
- Waktu yang telah diedit: 17 Februari 2023, 21:28 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerPipelinesIntegrations`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
        "lambda:DeleteFunction",
        "lambda:GetFunction",
        "lambda:InvokeFunction",
        "lambda:UpdateFunctionCode"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*sagemaker*",
        "arn:aws:lambda:*:*:function:*sageMaker*",
        "arn:aws:lambda:*:*:function:*SageMaker*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:CreateQueue",
        "sqs:SendMessage"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:*sagemaker*",
        "arn:aws:sqs:*:*:*sageMaker*",
        "arn:aws:sqs:*:*:*SageMaker*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lambda.amazonaws.com",
            "elasticmapreduce.amazonaws.com",
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:PutRule",
```

```
        "events:PutTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/SageMakerPipelineExecutionEMRStepStatusUpdateRule",
        "arn:aws:events:*:*:rule/SageMakerPipelineExecutionEMRClusterStatusUpdateRule"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:AddJobFlowSteps",
        "elasticmapreduce:CancelSteps",
        "elasticmapreduce:DescribeStep",
        "elasticmapreduce:RunJobFlow",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:TerminateJobFlows",
        "elasticmapreduce:ListSteps"
      ],
      "Resource" : [
        "arn:aws:elasticmapreduce:*:*:cluster/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSageMakerQuickSightVPCPolicy

Deskripsi: Kebijakan ini akan digunakan oleh SageMaker Unified Studios untuk membuat sumber daya terkait VPC QuickSight

`AmazonSageMakerQuickSightVPCPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerQuickSightVPCPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 03 Juni 2025, 17:37 UTC
- Waktu yang telah diedit: 03 Juni 2025, 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerQuickSightVPCPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSageMakerReadOnly

Deskripsi: Menyediakan akses baca saja ke Amazon SageMaker melalui AWS Management Console dan SDK.

`AmazonSageMakerReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerReadOnly` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 November 2017, 13:07 UTC
- Waktu yang telah diedit: 01 Desember 2021, 16:29 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerReadOnly`

Versi kebijakan

Versi kebijakan: v11 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:Describe*",
        "sagemaker:List*",
        "sagemaker:BatchGetMetrics",
        "sagemaker:GetDeviceRegistration",
        "sagemaker:GetDeviceFleetReport",
        "sagemaker:GetSearchSuggestions",
        "sagemaker:BatchGetRecord",
        "sagemaker:GetRecord",
        "sagemaker:Search",
        "sagemaker:QueryLineage",
        "sagemaker:GetLineageGroupPolicy",
        "sagemaker:BatchDescribeModelPackage",
        "sagemaker:GetModelPackageGroupPolicy"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "aws-marketplace:ViewSubscriptions",
        "cloudwatch:DescribeAlarms",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:ListGroups",
        "cognito-idp:ListIdentityProviders",
        "cognito-idp:ListUserPoolClients",
        "cognito-idp:ListUserPools",
        "cognito-idp:ListUsers",
        "cognito-idp:ListUsersInGroup",
        "ecr:Describe*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePoli

Deskripsi: Kebijakan peran layanan yang digunakan oleh AWS APIGateway dalam produk yang AWS ServiceCatalog disediakan dari SageMaker portofolio produk Amazon. Memberikan izin ke serangkaian layanan terkait termasuk CloudWatch Log dan lainnya.

`AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 25 Maret 2022, 04:25 UTC
- Waktu yang telah diedit: 25 Maret 2022, 04.25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DeleteLogDelivery",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:DescribeResourcePolicies",
        "logs:DescribeDestinations",
        "logs:DescribeExportTasks",
        "logs:DescribeMetricFilters",
        "logs:DescribeQueries",
        "logs:DescribeQueryDefinitions",
        "logs:DescribeSubscriptionFilters",
        "logs:GetLogDelivery",
        "logs:GetLogEvents",
        "logs:PutLogEvents",
        "logs:PutResourcePolicy",
        "logs:UpdateLogDelivery"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/apigateway/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSageMakerServiceCatalogProductsCloudformationServiceRoleP

Deskripsi: Kebijakan peran layanan yang digunakan oleh AWS CloudFormation dalam produk yang AWS ServiceCatalog disediakan dari SageMaker portofolio produk Amazon. Memberikan izin untuk subset layanan terkait termasuk SageMaker dan lainnya.

`AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 25 Maret 2022, 04:26 UTC
- Waktu yang telah diedit: 25 Maret 2022, 04.26 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
        "sagemaker:AddAssociation",
        "sagemaker:AddTags",
        "sagemaker:AssociateTrialComponent",
        "sagemaker:BatchDescribeModelPackage",
        "sagemaker:BatchGetMetrics",
        "sagemaker:BatchGetRecord",
        "sagemaker:BatchPutMetrics",
        "sagemaker:CreateAction",
        "sagemaker:CreateAlgorithm",
        "sagemaker:CreateApp",
        "sagemaker:CreateAppImageConfig",
        "sagemaker:CreateArtifact",
        "sagemaker:CreateAutoMLJob",
        "sagemaker:CreateCodeRepository",
        "sagemaker:CreateCompilationJob",
        "sagemaker:CreateContext",
        "sagemaker:CreateDataQualityJobDefinition",
        "sagemaker:CreateDeviceFleet",
        "sagemaker:CreateDomain",
        "sagemaker:CreateEdgePackagingJob",
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateExperiment",
        "sagemaker:CreateFeatureGroup",
        "sagemaker:CreateFlowDefinition",
        "sagemaker:CreateHumanTaskUi",
        "sagemaker:CreateHyperParameterTuningJob",
        "sagemaker:CreateImage",
        "sagemaker:CreateImageVersion",
        "sagemaker:CreateInferenceRecommendationsJob",
        "sagemaker:CreateLabelingJob",
        "sagemaker:CreateLineageGroupPolicy",
        "sagemaker:CreateModel",
        "sagemaker:CreateModelBiasJobDefinition",
        "sagemaker:CreateModelExplainabilityJobDefinition",
        "sagemaker:CreateModelPackage",
        "sagemaker:CreateModelPackageGroup",
        "sagemaker:CreateModelQualityJobDefinition",
        "sagemaker:CreateMonitoringSchedule",
        "sagemaker:CreateNotebookInstance",
        "sagemaker:CreateNotebookInstanceLifecycleConfig",
        "sagemaker:CreatePipeline",
        "sagemaker:CreatePresignedDomainUrl",
        "sagemaker:CreatePresignedNotebookInstanceUrl",
```

```
        "sagemaker:CreateProcessingJob",
        "sagemaker:CreateProject",
        "sagemaker:CreateTrainingJob",
        "sagemaker:CreateTransformJob",
        "sagemaker:CreateTrial",
        "sagemaker:CreateTrialComponent",
        "sagemaker:CreateUserProfile",
        "sagemaker:CreateWorkforce",
        "sagemaker:CreateWorkteam",
        "sagemaker:DeleteAction",
        "sagemaker:DeleteAlgorithm",
        "sagemaker:DeleteApp",
        "sagemaker:DeleteAppImageConfig",
        "sagemaker:DeleteArtifact",
        "sagemaker:DeleteAssociation",
        "sagemaker:DeleteCodeRepository",
        "sagemaker:DeleteContext",
        "sagemaker:DeleteDataQualityJobDefinition",
        "sagemaker:DeleteDeviceFleet",
        "sagemaker:DeleteDomain",
        "sagemaker:DeleteEndpoint",
        "sagemaker:DeleteEndpointConfig",
        "sagemaker:DeleteExperiment",
        "sagemaker:DeleteFeatureGroup",
        "sagemaker:DeleteFlowDefinition",
        "sagemaker:DeleteHumanLoop",
        "sagemaker:DeleteHumanTaskUi",
        "sagemaker:DeleteImage",
        "sagemaker:DeleteImageVersion",
        "sagemaker:DeleteLineageGroupPolicy",
        "sagemaker:DeleteModel",
        "sagemaker:DeleteModelBiasJobDefinition",
        "sagemaker:DeleteModelExplainabilityJobDefinition",
        "sagemaker:DeleteModelPackage",
        "sagemaker:DeleteModelPackageGroup",
        "sagemaker:DeleteModelPackageGroupPolicy",
        "sagemaker:DeleteModelQualityJobDefinition",
        "sagemaker:DeleteMonitoringSchedule",
        "sagemaker:DeleteNotebookInstance",
        "sagemaker:DeleteNotebookInstanceLifecycleConfig",
        "sagemaker:DeletePipeline",
        "sagemaker:DeleteProject",
        "sagemaker:DeleteRecord",
        "sagemaker:DeleteTags",
```

```
        "sagemaker:DeleteTrial",
        "sagemaker:DeleteTrialComponent",
        "sagemaker:DeleteUserProfile",
        "sagemaker:DeleteWorkforce",
        "sagemaker:DeleteWorkteam",
        "sagemaker:DeregisterDevices",
        "sagemaker:DescribeAction",
        "sagemaker:DescribeAlgorithm",
        "sagemaker:DescribeApp",
        "sagemaker:DescribeAppImageConfig",
        "sagemaker:DescribeArtifact",
        "sagemaker:DescribeAutoMLJob",
        "sagemaker:DescribeCodeRepository",
        "sagemaker:DescribeCompilationJob",
        "sagemaker:DescribeContext",
        "sagemaker:DescribeDataQualityJobDefinition",
        "sagemaker:DescribeDevice",
        "sagemaker:DescribeDeviceFleet",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeEdgePackagingJob",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeExperiment",
        "sagemaker:DescribeFeatureGroup",
        "sagemaker:DescribeFlowDefinition",
        "sagemaker:DescribeHumanLoop",
        "sagemaker:DescribeHumanTaskUi",
        "sagemaker:DescribeHyperParameterTuningJob",
        "sagemaker:DescribeImage",
        "sagemaker:DescribeImageVersion",
        "sagemaker:DescribeInferenceRecommendationsJob",
        "sagemaker:DescribeLabelingJob",
        "sagemaker:DescribeLineageGroup",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeModelBiasJobDefinition",
        "sagemaker:DescribeModelExplainabilityJobDefinition",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribeModelQualityJobDefinition",
        "sagemaker:DescribeMonitoringSchedule",
        "sagemaker:DescribeNotebookInstance",
        "sagemaker:DescribeNotebookInstanceLifecycleConfig",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribePipelineDefinitionForExecution",
```

```
        "sagemaker:DescribePipelineExecution",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeProject",
        "sagemaker:DescribeSubscribedWorkteam",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:DescribeTransformJob",
        "sagemaker:DescribeTrial",
        "sagemaker:DescribeTrialComponent",
        "sagemaker:DescribeUserProfile",
        "sagemaker:DescribeWorkforce",
        "sagemaker:DescribeWorkteam",
        "sagemaker:DisableSagemakerServicecatalogPortfolio",
        "sagemaker:DisassociateTrialComponent",
        "sagemaker:EnableSagemakerServicecatalogPortfolio",
        "sagemaker:GetDeviceFleetReport",
        "sagemaker:GetDeviceRegistration",
        "sagemaker:GetLineageGroupPolicy",
        "sagemaker:GetModelPackageGroupPolicy",
        "sagemaker:GetRecord",
        "sagemaker:GetSagemakerServicecatalogPortfolioStatus",
        "sagemaker:GetSearchSuggestions",
        "sagemaker:InvokeEndpoint",
        "sagemaker:InvokeEndpointAsync",
        "sagemaker:ListActions",
        "sagemaker:ListAlgorithms",
        "sagemaker:ListAppImageConfigs",
        "sagemaker:ListApps",
        "sagemaker:ListArtifacts",
        "sagemaker:ListAssociations",
        "sagemaker:ListAutoMLJobs",
        "sagemaker:ListCandidatesForAutoMLJob",
        "sagemaker:ListCodeRepositories",
        "sagemaker:ListCompilationJobs",
        "sagemaker:ListContexts",
        "sagemaker:ListDataQualityJobDefinitions",
        "sagemaker:ListDeviceFleets",
        "sagemaker:ListDevices",
        "sagemaker:ListDomains",
        "sagemaker:ListEdgePackagingJobs",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListEndpoints",
        "sagemaker:ListExperiments",
        "sagemaker:ListFeatureGroups",
        "sagemaker:ListFlowDefinitions",
```

```
        "sagemaker:ListHumanLoops",
        "sagemaker:ListHumanTaskUis",
        "sagemaker:ListHyperParameterTuningJobs",
        "sagemaker:ListImageVersions",
        "sagemaker:ListImages",
        "sagemaker:ListInferenceRecommendationsJobs",
        "sagemaker:ListLabelingJobs",
        "sagemaker:ListLabelingJobsForWorkteam",
        "sagemaker:ListLineageGroups",
        "sagemaker:ListModelBiasJobDefinitions",
        "sagemaker:ListModelExplainabilityJobDefinitions",
        "sagemaker:ListModelMetadata",
        "sagemaker:ListModelPackageGroups",
        "sagemaker:ListModelPackages",
        "sagemaker:ListModelQualityJobDefinitions",
        "sagemaker:ListModels",
        "sagemaker:ListMonitoringExecutions",
        "sagemaker:ListMonitoringSchedules",
        "sagemaker:ListNotebookInstanceLifecycleConfigs",
        "sagemaker:ListNotebookInstances",
        "sagemaker:ListPipelineExecutionSteps",
        "sagemaker:ListPipelineExecutions",
        "sagemaker:ListPipelineParametersForExecution",
        "sagemaker:ListPipelines",
        "sagemaker:ListProcessingJobs",
        "sagemaker:ListProjects",
        "sagemaker:ListSubscribedWorkteams",
        "sagemaker:ListTags",
        "sagemaker:ListTrainingJobs",
        "sagemaker:ListTrainingJobsForHyperParameterTuningJob",
        "sagemaker:ListTransformJobs",
        "sagemaker:ListTrialComponents",
        "sagemaker:ListTrials",
        "sagemaker:ListUserProfiles",
        "sagemaker:ListWorkforces",
        "sagemaker:ListWorkteams",
        "sagemaker:PutLineageGroupPolicy",
        "sagemaker:PutModelPackageGroupPolicy",
        "sagemaker:PutRecord",
        "sagemaker:QueryLineage",
        "sagemaker:RegisterDevices",
        "sagemaker:RenderUiTemplate",
        "sagemaker:Search",
        "sagemaker:SendHeartbeat",
```

```
        "sagemaker:SendPipelineExecutionStepFailure",
        "sagemaker:SendPipelineExecutionStepSuccess",
        "sagemaker:StartHumanLoop",
        "sagemaker:StartMonitoringSchedule",
        "sagemaker:StartNotebookInstance",
        "sagemaker:StartPipelineExecution",
        "sagemaker:StopAutoMLJob",
        "sagemaker:StopCompilationJob",
        "sagemaker:StopEdgePackagingJob",
        "sagemaker:StopHumanLoop",
        "sagemaker:StopHyperParameterTuningJob",
        "sagemaker:StopInferenceRecommendationsJob",
        "sagemaker:StopLabelingJob",
        "sagemaker:StopMonitoringSchedule",
        "sagemaker:StopNotebookInstance",
        "sagemaker:StopPipelineExecution",
        "sagemaker:StopProcessingJob",
        "sagemaker:StopTrainingJob",
        "sagemaker:StopTransformJob",
        "sagemaker:UpdateAction",
        "sagemaker:UpdateAppImageConfig",
        "sagemaker:UpdateArtifact",
        "sagemaker:UpdateCodeRepository",
        "sagemaker:UpdateContext",
        "sagemaker:UpdateDeviceFleet",
        "sagemaker:UpdateDevices",
        "sagemaker:UpdateDomain",
        "sagemaker:UpdateEndpoint",
        "sagemaker:UpdateEndpointWeightsAndCapacities",
        "sagemaker:UpdateExperiment",
        "sagemaker:UpdateImage",
        "sagemaker:UpdateModelPackage",
        "sagemaker:UpdateMonitoringSchedule",
        "sagemaker:UpdateNotebookInstance",
        "sagemaker:UpdateNotebookInstanceLifecycleConfig",
        "sagemaker:UpdatePipeline",
        "sagemaker:UpdatePipelineExecution",
        "sagemaker:UpdateProject",
        "sagemaker:UpdateTrainingJob",
        "sagemaker:UpdateTrial",
        "sagemaker:UpdateTrialComponent",
        "sagemaker:UpdateUserProfile",
        "sagemaker:UpdateWorkforce",
        "sagemaker:UpdateWorkteam"
```

```
      ],
      "NotResource" : [
        "arn:aws:sagemaker:*:*:domain/*",
        "arn:aws:sagemaker:*:*:user-profile/*",
        "arn:aws:sagemaker:*:*:app/*",
        "arn:aws:sagemaker:*:*:flow-definition/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsCodeBuildRole",
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsExecutionRole"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy

Deskripsi: Kebijakan peran layanan yang digunakan oleh AWS CodeBuild dalam produk yang AWS ServiceCatalog disediakan dari SageMaker portofolio produk Amazon. Memberikan izin untuk subset layanan terkait termasuk CodePipeline, CodeBuild dan lainnya.

`AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 25 Maret 2022, 04:27 UTC
- Waktu yang telah diedit: 11 Juni 2024, 18:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonSageMakerCodeBuildCodeCommitPermission",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:CancelUploadArchive",
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetUploadArchiveStatus",
        "codecommit:UploadArchive"
      ],
      "Resource" : "arn:aws:codecommit:*:*:sagemaker-*"
    },
    {
```

```
      "Sid" : "AmazonSageMakerCodeBuildECRReadPermission",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:DescribeImageScanFindings",
        "ecr:DescribeRegistry",
        "ecr:DescribeImageReplicationStatus",
        "ecr:DescribeRepositories",
        "ecr:DescribeImageReplicationStatus",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerCodeBuildECRWritePermission",
      "Effect" : "Allow",
      "Action" : [
        "ecr:CompleteLayerUpload",
        "ecr:CreateRepository",
        "ecr:InitiateLayerUpload",
        "ecr:PutImage",
        "ecr:UploadLayerPart"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerCodeBuildPassRoletPermission",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsEventsRole",
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsCodePipelineRole",
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsCloudformationRole",
```

```
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsCodeBuildRole",
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsExecutionRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "events.amazonaws.com",
            "codepipeline.amazonaws.com",
            "cloudformation.amazonaws.com",
            "codebuild.amazonaws.com",
            "sagemaker.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerCodeBuildLogPermission",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DeleteLogDelivery",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:DescribeResourcePolicies",
        "logs:DescribeDestinations",
        "logs:DescribeExportTasks",
        "logs:DescribeMetricFilters",
        "logs:DescribeQueries",
        "logs:DescribeQueryDefinitions",
        "logs:DescribeSubscriptionFilters",
        "logs:GetLogDelivery",
        "logs:GetLogEvents",
        "logs:ListLogDeliveries",
        "logs:PutLogEvents",
        "logs:PutResourcePolicy",
        "logs:UpdateLogDelivery"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/codebuild/*"
    },
    {
```

```
      "Sid" : "AmazonSageMakerCodeBuildS3Permission",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:GetBucketAcl",
        "s3:GetBucketCors",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:PutBucketCors",
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*",
        "arn:aws:s3:::sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerCodeBuildSageMakerPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddAssociation",
        "sagemaker:AddTags",
        "sagemaker:AssociateTrialComponent",
        "sagemaker:BatchDescribeModelPackage",
        "sagemaker:BatchGetMetrics",
        "sagemaker:BatchGetRecord",
        "sagemaker:BatchPutMetrics",
        "sagemaker:CreateAction",
        "sagemaker:CreateAlgorithm",
        "sagemaker:CreateApp",
        "sagemaker:CreateAppImageConfig",
        "sagemaker:CreateArtifact",
        "sagemaker:CreateAutoMLJob",
        "sagemaker:CreateCodeRepository",
        "sagemaker:CreateCompilationJob",
        "sagemaker:CreateContext",
        "sagemaker:CreateDataQualityJobDefinition",
```

```
        "sagemaker:CreateDeviceFleet",
        "sagemaker:CreateDomain",
        "sagemaker:CreateEdgePackagingJob",
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateExperiment",
        "sagemaker:CreateFeatureGroup",
        "sagemaker:CreateFlowDefinition",
        "sagemaker:CreateHumanTaskUi",
        "sagemaker:CreateHyperParameterTuningJob",
        "sagemaker:CreateImage",
        "sagemaker:CreateImageVersion",
        "sagemaker:CreateInferenceRecommendationsJob",
        "sagemaker:CreateLabelingJob",
        "sagemaker:CreateLineageGroupPolicy",
        "sagemaker:CreateModel",
        "sagemaker:CreateModelBiasJobDefinition",
        "sagemaker:CreateModelExplainabilityJobDefinition",
        "sagemaker:CreateModelPackage",
        "sagemaker:CreateModelPackageGroup",
        "sagemaker:CreateModelQualityJobDefinition",
        "sagemaker:CreateMonitoringSchedule",
        "sagemaker:CreateNotebookInstance",
        "sagemaker:CreateNotebookInstanceLifecycleConfig",
        "sagemaker:CreatePipeline",
        "sagemaker:CreatePresignedDomainUrl",
        "sagemaker:CreatePresignedNotebookInstanceUrl",
        "sagemaker:CreateProcessingJob",
        "sagemaker:CreateProject",
        "sagemaker:CreateTrainingJob",
        "sagemaker:CreateTransformJob",
        "sagemaker:CreateTrial",
        "sagemaker:CreateTrialComponent",
        "sagemaker:CreateUserProfile",
        "sagemaker:CreateWorkforce",
        "sagemaker:CreateWorkteam",
        "sagemaker:DeleteAction",
        "sagemaker:DeleteAlgorithm",
        "sagemaker:DeleteApp",
        "sagemaker:DeleteAppImageConfig",
        "sagemaker:DeleteArtifact",
        "sagemaker:DeleteAssociation",
        "sagemaker:DeleteCodeRepository",
        "sagemaker:DeleteContext",
```

```
        "sagemaker:DeleteDataQualityJobDefinition",
        "sagemaker:DeleteDeviceFleet",
        "sagemaker:DeleteDomain",
        "sagemaker:DeleteEndpoint",
        "sagemaker:DeleteEndpointConfig",
        "sagemaker:DeleteExperiment",
        "sagemaker:DeleteFeatureGroup",
        "sagemaker:DeleteFlowDefinition",
        "sagemaker:DeleteHumanLoop",
        "sagemaker:DeleteHumanTaskUi",
        "sagemaker:DeleteImage",
        "sagemaker:DeleteImageVersion",
        "sagemaker:DeleteLineageGroupPolicy",
        "sagemaker:DeleteModel",
        "sagemaker:DeleteModelBiasJobDefinition",
        "sagemaker:DeleteModelExplainabilityJobDefinition",
        "sagemaker:DeleteModelPackage",
        "sagemaker:DeleteModelPackageGroup",
        "sagemaker:DeleteModelPackageGroupPolicy",
        "sagemaker:DeleteModelQualityJobDefinition",
        "sagemaker:DeleteMonitoringSchedule",
        "sagemaker:DeleteNotebookInstance",
        "sagemaker:DeleteNotebookInstanceLifecycleConfig",
        "sagemaker:DeletePipeline",
        "sagemaker:DeleteProject",
        "sagemaker:DeleteRecord",
        "sagemaker:DeleteTags",
        "sagemaker:DeleteTrial",
        "sagemaker:DeleteTrialComponent",
        "sagemaker:DeleteUserProfile",
        "sagemaker:DeleteWorkforce",
        "sagemaker:DeleteWorkteam",
        "sagemaker:DeregisterDevices",
        "sagemaker:DescribeAction",
        "sagemaker:DescribeAlgorithm",
        "sagemaker:DescribeApp",
        "sagemaker:DescribeAppImageConfig",
        "sagemaker:DescribeArtifact",
        "sagemaker:DescribeAutoMLJob",
        "sagemaker:DescribeCodeRepository",
        "sagemaker:DescribeCompilationJob",
        "sagemaker:DescribeContext",
        "sagemaker:DescribeDataQualityJobDefinition",
        "sagemaker:DescribeDevice",
```

```
        "sagemaker:DescribeDeviceFleet",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeEdgePackagingJob",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeExperiment",
        "sagemaker:DescribeFeatureGroup",
        "sagemaker:DescribeFlowDefinition",
        "sagemaker:DescribeHumanLoop",
        "sagemaker:DescribeHumanTaskUi",
        "sagemaker:DescribeHyperParameterTuningJob",
        "sagemaker:DescribeImage",
        "sagemaker:DescribeImageVersion",
        "sagemaker:DescribeInferenceRecommendationsJob",
        "sagemaker:DescribeLabelingJob",
        "sagemaker:DescribeLineageGroup",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeModelBiasJobDefinition",
        "sagemaker:DescribeModelExplainabilityJobDefinition",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribeModelQualityJobDefinition",
        "sagemaker:DescribeMonitoringSchedule",
        "sagemaker:DescribeNotebookInstance",
        "sagemaker:DescribeNotebookInstanceLifecycleConfig",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribePipelineDefinitionForExecution",
        "sagemaker:DescribePipelineExecution",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeProject",
        "sagemaker:DescribeSubscribedWorkteam",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:DescribeTransformJob",
        "sagemaker:DescribeTrial",
        "sagemaker:DescribeTrialComponent",
        "sagemaker:DescribeUserProfile",
        "sagemaker:DescribeWorkforce",
        "sagemaker:DescribeWorkteam",
        "sagemaker:DisableSagemakerServicecatalogPortfolio",
        "sagemaker:DisassociateTrialComponent",
        "sagemaker:EnableSagemakerServicecatalogPortfolio",
        "sagemaker:GetDeviceFleetReport",
        "sagemaker:GetDeviceRegistration",
        "sagemaker:GetLineageGroupPolicy",
```

```
        "sagemaker:GetModelPackageGroupPolicy",
        "sagemaker:GetRecord",
        "sagemaker:GetSagemakerServicecatalogPortfolioStatus",
        "sagemaker:GetSearchSuggestions",
        "sagemaker:InvokeEndpoint",
        "sagemaker:InvokeEndpointAsync",
        "sagemaker:ListActions",
        "sagemaker:ListAlgorithms",
        "sagemaker:ListAppImageConfigs",
        "sagemaker:ListApps",
        "sagemaker:ListArtifacts",
        "sagemaker:ListAssociations",
        "sagemaker:ListAutoMLJobs",
        "sagemaker:ListCandidatesForAutoMLJob",
        "sagemaker:ListCodeRepositories",
        "sagemaker:ListCompilationJobs",
        "sagemaker:ListContexts",
        "sagemaker:ListDataQualityJobDefinitions",
        "sagemaker:ListDeviceFleets",
        "sagemaker:ListDevices",
        "sagemaker:ListDomains",
        "sagemaker:ListEdgePackagingJobs",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListEndpoints",
        "sagemaker:ListExperiments",
        "sagemaker:ListFeatureGroups",
        "sagemaker:ListFlowDefinitions",
        "sagemaker:ListHumanLoops",
        "sagemaker:ListHumanTaskUis",
        "sagemaker:ListHyperParameterTuningJobs",
        "sagemaker:ListImageVersions",
        "sagemaker:ListImages",
        "sagemaker:ListInferenceRecommendationsJobs",
        "sagemaker:ListLabelingJobs",
        "sagemaker:ListLabelingJobsForWorkteam",
        "sagemaker:ListLineageGroups",
        "sagemaker:ListModelBiasJobDefinitions",
        "sagemaker:ListModelExplainabilityJobDefinitions",
        "sagemaker:ListModelMetadata",
        "sagemaker:ListModelPackageGroups",
        "sagemaker:ListModelPackages",
        "sagemaker:ListModelQualityJobDefinitions",
        "sagemaker:ListModels",
        "sagemaker:ListMonitoringExecutions",
```

```
        "sagemaker:ListMonitoringSchedules",
        "sagemaker:ListNotebookInstanceLifecycleConfigs",
        "sagemaker:ListNotebookInstances",
        "sagemaker:ListPipelineExecutionSteps",
        "sagemaker:ListPipelineExecutions",
        "sagemaker:ListPipelineParametersForExecution",
        "sagemaker:ListPipelines",
        "sagemaker:ListProcessingJobs",
        "sagemaker:ListProjects",
        "sagemaker:ListSubscribedWorkteams",
        "sagemaker:ListTags",
        "sagemaker:ListTrainingJobs",
        "sagemaker:ListTrainingJobsForHyperParameterTuningJob",
        "sagemaker:ListTransformJobs",
        "sagemaker:ListTrialComponents",
        "sagemaker:ListTrials",
        "sagemaker:ListUserProfiles",
        "sagemaker:ListWorkforces",
        "sagemaker:ListWorkteams",
        "sagemaker:PutLineageGroupPolicy",
        "sagemaker:PutModelPackageGroupPolicy",
        "sagemaker:PutRecord",
        "sagemaker:QueryLineage",
        "sagemaker:RegisterDevices",
        "sagemaker:RenderUiTemplate",
        "sagemaker:Search",
        "sagemaker:SendHeartbeat",
        "sagemaker:SendPipelineExecutionStepFailure",
        "sagemaker:SendPipelineExecutionStepSuccess",
        "sagemaker:StartHumanLoop",
        "sagemaker:StartMonitoringSchedule",
        "sagemaker:StartNotebookInstance",
        "sagemaker:StartPipelineExecution",
        "sagemaker:StopAutoMLJob",
        "sagemaker:StopCompilationJob",
        "sagemaker:StopEdgePackagingJob",
        "sagemaker:StopHumanLoop",
        "sagemaker:StopHyperParameterTuningJob",
        "sagemaker:StopInferenceRecommendationsJob",
        "sagemaker:StopLabelingJob",
        "sagemaker:StopMonitoringSchedule",
        "sagemaker:StopNotebookInstance",
        "sagemaker:StopPipelineExecution",
        "sagemaker:StopProcessingJob",
```

```
        "sagemaker:StopTrainingJob",
        "sagemaker:StopTransformJob",
        "sagemaker:UpdateAction",
        "sagemaker:UpdateAppImageConfig",
        "sagemaker:UpdateArtifact",
        "sagemaker:UpdateCodeRepository",
        "sagemaker:UpdateContext",
        "sagemaker:UpdateDeviceFleet",
        "sagemaker:UpdateDevices",
        "sagemaker:UpdateDomain",
        "sagemaker:UpdateEndpoint",
        "sagemaker:UpdateEndpointWeightsAndCapacities",
        "sagemaker:UpdateExperiment",
        "sagemaker:UpdateImage",
        "sagemaker:UpdateModelPackage",
        "sagemaker:UpdateMonitoringSchedule",
        "sagemaker:UpdateNotebookInstance",
        "sagemaker:UpdateNotebookInstanceLifecycleConfig",
        "sagemaker:UpdatePipeline",
        "sagemaker:UpdatePipelineExecution",
        "sagemaker:UpdateProject",
        "sagemaker:UpdateTrainingJob",
        "sagemaker:UpdateTrial",
        "sagemaker:UpdateTrialComponent",
        "sagemaker:UpdateUserProfile",
        "sagemaker:UpdateWorkforce",
        "sagemaker:UpdateWorkteam"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:model/*",
        "arn:aws:sagemaker:*:*:pipeline/*",
        "arn:aws:sagemaker:*:*:project/*",
        "arn:aws:sagemaker:*:*:model-package/*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerCodeBuildCodeStarConnectionPermission",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection"
      ],
      "Resource" : [
```

```
        "arn:aws:codestar-connections:*:*:connection/*"
      ],
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "aws:ResourceTag/sagemaker" : "true"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerCodeBuildCodeConnectionPermission",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:UseConnection"
      ],
      "Resource" : [
        "arn:aws:codeconnections:*:*:connection/*"
      ],
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "aws:ResourceTag/sagemaker" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePo

Deskripsi: Kebijakan peran layanan yang digunakan oleh AWS CodePipeline dalam produk yang AWS ServiceCatalog disediakan dari SageMaker portofolio produk Amazon. Memberikan izin untuk subset layanan terkait termasuk CodePipeline, CodeBuild dan lainnya.

`AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 22 Februari 2022, 09:53 UTC
- Waktu yang telah diedit: 11 Juni 2024, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonSageMakerCodePipelineCFnPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:CreateStack",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
```

```
        "cloudformation:ExecuteChangeSet",
        "cloudformation:SetStackPolicy",
        "cloudformation:UpdateStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/sagemaker-*"
    },
    {
      "Sid" : "AmazonSageMakerCodePipelineCFnTagPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/sagemaker-*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "sagemaker:project-name"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerCodePipelineS3Permission",
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerCodePipelinePassRolePermission",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
```

```
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsCloudformationRole"
      ]
    },
    {
      "Sid" : "AmazonSageMakerCodePipelineCodeBuildPermission",
      "Effect" : "Allow",
      "Action" : [
        "codebuild:BatchGetBuilds",
        "codebuild:StartBuild"
      ],
      "Resource" : [
        "arn:aws:codebuild:*:*:project/sagemaker-*",
        "arn:aws:codebuild:*:*:build/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerCodePipelineCodeCommitPermission",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:CancelUploadArchive",
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetUploadArchiveStatus",
        "codecommit:UploadArchive"
      ],
      "Resource" : "arn:aws:codecommit:*:*:sagemaker-*"
    },
    {
      "Sid" : "AmazonSageMakerCodePipelineCodeStarConnectionPermission",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection"
      ],
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*"
      ],
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "aws:ResourceTag/sagemaker" : "true"
        }
      }
    },
    {
```

```
      "Sid" : "AmazonSageMakerCodePipelineCodeConnectionPermission",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:UseConnection"
      ],
      "Resource" : [
        "arn:aws:codeconnections:*:*:connection/*"
      ],
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "aws:ResourceTag/sagemaker" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy

Deskripsi: Kebijakan peran layanan yang digunakan oleh AWS CloudWatch Acara dalam produk yang AWS ServiceCatalog disediakan dari SageMaker portofolio produk Amazon. Memberikan izin untuk subset layanan terkait termasuk CodePipeline dan lainnya.

`AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 22 Februari 2022, 09:53 UTC
- Waktu telah diedit: 22 Februari 2022, 09:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy

Deskripsi: Kebijakan peran layanan yang digunakan oleh AWS Firehose dalam produk yang AWS ServiceCatalog disediakan dari portofolio produk Amazon SageMaker . Memberikan izin ke serangkaian layanan terkait termasuk Firehose dan lainnya.

`AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 22 Februari 2022, 09:54 UTC
- Waktu telah diedit: 22 Februari 2022, 09:54 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : "arn:aws:firehose:*:*:deliverystream/sagemaker-*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy

Deskripsi: Kebijakan peran layanan yang digunakan oleh AWS Glue dalam produk AWS ServiceCatalog yang disediakan dari SageMaker portofolio produk Amazon. Memberikan izin ke serangkaian layanan terkait termasuk Glue, S3, dan lainnya.

`AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 22 Februari 2022, 09:51 UTC
- Waktu yang telah diedit: 26 Agustus 2022 19.13 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:BatchCreatePartition",
        "glue:BatchDeletePartition",
        "glue:BatchDeleteTable",
        "glue:BatchDeleteTableVersion",
        "glue:BatchGetPartition",
        "glue:CreateDatabase",
        "glue:CreatePartition",
        "glue:CreateTable",
        "glue:DeletePartition",
        "glue:DeleteTable",
        "glue:DeleteTableVersion",
        "glue:GetDatabase",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetTableVersion",
        "glue:GetTableVersions",
        "glue:SearchTables",
        "glue:UpdatePartition",
        "glue:UpdateTable",
        "glue:GetUserDefinedFunctions"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/default",
        "arn:aws:glue:*:*:database/global_temp",
```

```
        "arn:aws:glue:*:*:database/sagemaker-*",
        "arn:aws:glue:*:*:table/sagemaker-*",
        "arn:aws:glue:*:*:tableVersion/sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:GetBucketAcl",
        "s3:GetBucketCors",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:PutBucketCors"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*",
        "arn:aws:s3:::sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*",
        "arn:aws:s3:::sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DeleteLogDelivery",
```

```
        "logs:Describe*",
        "logs:GetLogDelivery",
        "logs:GetLogEvents",
        "logs:ListLogDeliveries",
        "logs:PutLogEvents",
        "logs:PutResourcePolicy",
        "logs:UpdateLogDelivery"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/glue/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy

Deskripsi: Kebijakan peran layanan yang digunakan oleh AWS Lambda dalam produk yang AWS ServiceCatalog disediakan dari portofolio produk Amazon SageMaker . Memberikan izin ke serangkaian layanan terkait termasuk ECR, S3, dan lainnya.

`AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 04 April 2022, 16:34 UTC

- Waktu yang telah diedit: 11 Juni 2024, 18:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSageMakerTrainingPlanCreateAccess

Deskripsi: Kebijakan Terkelola Amazon ini memberikan izin yang diperlukan untuk membuat dan mengelola Rencana SageMaker Pelatihan. Ini memungkinkan pengguna untuk membuat Rencana Pelatihan dan Kapasitas Cadangan, menjelaskan Rencana Pelatihan yang ada, dan melakukan operasi pencarian dan daftar.

`AmazonSageMakerTrainingPlanCreateAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerTrainingPlanCreateAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 04 Desember 2024, 13:21 UTC

- Waktu telah diedit: 04 Desember 2024, 13:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerTrainingPlanCreateAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateTrainingPlanPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateTrainingPlan",
        "sagemaker:CreateReservedCapacity"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-plan/*",
        "arn:aws:sagemaker:*:*:reserved-capacity/*"
      ]
    },
    {
      "Sid" : "AggTagsToTrainingPlanPermissions",
      "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" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSecurityLakeAdministrator

Deskripsi: Menyediakan akses penuh ke Amazon Security Lake dan layanan terkait yang diperlukan untuk mengelola Security Lake.

`AmazonSecurityLakeAdministrator`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSecurityLakeAdministrator` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 Mei 2023, 22:04 UTC
- Waktu telah diedit: 23 Februari 2024, 16:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSecurityLakeAdministrator`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowActionsWithAnyResource",
      "Effect" : "Allow",
      "Action" : [
        "securitylake:*",
        "organizations:DescribeOrganization",
        "organizations:ListDelegatedServicesForAccount",
        "organizations:ListAccounts",
        "iam:ListRoles",
        "ram:GetResourceShareAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsWithAnyResourceViaSecurityLake",
```

```
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateCrawler",
        "glue:StopCrawlerSchedule",
        "lambda:CreateEventSourceMapping",
        "lakeformation:GrantPermissions",
        "lakeformation:ListPermissions",
        "lakeformation:RegisterResource",
        "lakeformation:RevokePermissions",
        "lakeformation:GetDatalakeSettings",
        "events:ListConnections",
        "events:ListApiDestinations",
        "iam:GetRole",
        "iam:ListAttachedRolePolicies",
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowManagingSecurityLakeS3Buckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutBucketPolicy",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketNotification",
        "s3:PutBucketTagging",
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketVersioning",
        "s3:PutReplicationConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:GetBucketNotification"
      ],
      "Resource" : "arn:aws:s3:::aws-security-data-lake*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
```

```
        }
      }
    },
    {
      "Sid" : "AllowLambdaCreateFunction",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*",
        "arn:aws:lambda:*:*:function:AmazonSecurityLake*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowLambdaAddPermission",
      "Effect" : "Allow",
      "Action" : [
        "lambda:AddPermission"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*",
        "arn:aws:lambda:*:*:function:AmazonSecurityLake*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        },
        "StringEquals" : {
          "lambda:Principal" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowGlueActions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:GetDatabase",
```

```
        "glue:CreateTable",
        "glue:GetTable"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/amazon_security_lake_glue_db*",
        "arn:aws:glue:*:*:table/amazon_security_lake_glue_db*/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowEventBridgeActions",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:PutRule",
        "events:DescribeRule",
        "events:CreateApiDestination",
        "events:CreateConnection",
        "events:UpdateConnection",
        "events:UpdateApiDestination",
        "events:DeleteConnection",
        "events:DeleteApiDestination",
        "events:ListTargetsByRule",
        "events:RemoveTargets",
        "events:DeleteRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/AmazonSecurityLake*",
        "arn:aws:events:*:*:rule/SecurityLake*",
        "arn:aws:events:*:*:api-destination/AmazonSecurityLake*",
        "arn:aws:events:*:*:connection/AmazonSecurityLake*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
```

```
      "Sid" : "AllowSQSActions",
      "Effect" : "Allow",
      "Action" : [
        "sqs:CreateQueue",
        "sqs:SetQueueAttributes",
        "sqs:GetQueueURL",
        "sqs:AddPermission",
        "sqs:GetQueueAttributes",
        "sqs:DeleteQueue"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:SecurityLake*",
        "arn:aws:sqs:*:*:AmazonSecurityLake*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowKmsCmkGrantForSecurityLake",
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        },
        "StringLike" : {
          "kms:EncryptionContext:aws:s3:arn" : "arn:aws:s3:::aws-security-data-lake*"
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "GenerateDataKey",
            "RetireGrant",
            "Decrypt"
          ]
        }
      }
    },
    {
      "Sid" : "AllowEnablingQueryBasedSubscribers",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ram:CreateResourceShare",
        "ram:AssociateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "ram:ResourceArn" : [
            "arn:aws:glue:*:*:catalog",
            "arn:aws:glue:*:*:database/amazon_security_lake_glue_db*",
            "arn:aws:glue:*:*:table/amazon_security_lake_glue_db*/*"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowConfiguringQueryBasedSubscribers",
      "Effect" : "Allow",
      "Action" : [
        "ram:UpdateResourceShare",
        "ram:GetResourceShares",
        "ram:DisassociateResourceShare",
        "ram:DeleteResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ram:ResourceShareName" : "LakeFormation*"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowConfiguringCredentialsForSubscriberNotification",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue"
```

```
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:events!connection/
AmazonSecurityLake-*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleForUpdatingGluePartitionsSecLakeArn",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSecurityLakeMetaStoreManager",
        "arn:aws:iam::*:role/service-role/AmazonSecurityLakeMetaStoreManagerV2"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        },
        "StringLike" : {
          "iam:AssociatedResourceARN" : "arn:aws:securitylake:*:*:data-lake/default"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleForUpdatingGluePartitionsLambdaArn",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSecurityLakeMetaStoreManager",
        "arn:aws:iam::*:role/service-role/AmazonSecurityLakeMetaStoreManagerV2"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        },
        "StringLike" : {
          "iam:AssociatedResourceARN" : [
            "arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*",
            "arn:aws:lambda:*:*:function:AmazonSecurityLake*"
          ]
        },
```

```
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleForCrossRegionReplicationSecLakeArn",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeS3ReplicationRole",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "s3.amazonaws.com"
        },
        "StringLike" : {
          "iam:AssociatedResourceARN" : "arn:aws:securitylake:*:*:data-lake/default"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleForCrossRegionReplicationS3Arn",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeS3ReplicationRole",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "s3.amazonaws.com"
        },
        "StringLike" : {
          "iam:AssociatedResourceARN" : "arn:aws:s3:::aws-security-data-lake*"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleForCustomSourceCrawlerSecLakeArn",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeCustomDataGlueCrawler*",
```

```
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "glue.amazonaws.com"
        },
        "StringLike" : {
          "iam:AssociatedResourceARN" : "arn:aws:securitylake:*:*:data-lake/default"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleForCustomSourceCrawlerGlueArn",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeCustomDataGlueCrawler*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "glue.amazonaws.com"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleForSubscriberNotificationSecLakeArn",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeSubscriberEventBridge",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "events.amazonaws.com"
        },
        "StringLike" : {
          "iam:AssociatedResourceARN" : "arn:aws:securitylake:*:*:subscriber/*"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleForSubscriberNotificationEventsArn",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
```

```
      "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeSubscriberEventBridge",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "events.amazonaws.com"
        },
        "StringLike" : {
          "iam:AssociatedResourceARN" : "arn:aws:events:*:*:rule/AmazonSecurityLake*"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowOnboardingToSecurityLakeDependencies",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/securitylake.amazonaws.com/
AWSServiceRoleForSecurityLake",
        "arn:aws:iam::*:role/aws-service-role/lakeformation.amazonaws.com/
AWSServiceRoleForLakeFormationDataAccess",
        "arn:aws:iam::*:role/aws-service-role/apidestinations.events.amazonaws.com/
AWSServiceRoleForAmazonEventBridgeApiDestinations"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : [
            "securitylake.amazonaws.com",
            "lakeformation.amazonaws.com",
            "apidestinations.events.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "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" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSecurityLakeMetastoreManager

Deskripsi: Kebijakan untuk Amazon SecurityLake meta store manager lambda yang memungkinkan akses ke cloudwatch, S3, Glue dan SQS.

`AmazonSecurityLakeMetastoreManager`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSecurityLakeMetastoreManager` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 23 Januari 2024, 15:26 UTC
- Waktu yang telah diedit: 01 April 2024, 20:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSecurityLakeMetastoreManager`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowWriteLambdaLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/lambda/AmazonSecurityLake*",
        "arn:aws:logs:*:*:/aws/lambda/AmazonSecurityLake*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowGlueManage",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreatePartition",
        "glue:BatchCreatePartition",
        "glue:GetTable",
        "glue:UpdateTable"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/amazon_security_lake_glue_db*/*",
        "arn:aws:glue:*:*:database/amazon_security_lake_glue_db*",
        "arn:aws:glue:*:*:catalog"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowToReadFromSqs",
      "Effect" : "Allow",
      "Action" : [
        "sqs:ReceiveMessage",
        "sqs:DeleteMessage",
        "sqs:GetQueueAttributes"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:AmazonSecurityLake*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowMetaDataReadWrite",
      "Effect" : "Allow",
```

```
      "Action" : [
        "s3:ListBucket",
        "s3:PutObject",
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-security-data-lake*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowMetaDataCleanup",
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-security-data-lake*/metadata/*.avro",
        "arn:aws:s3:::aws-security-data-lake*/metadata/*.metadata.json"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSecurityLakePermissionsBoundary

Deskripsi: Amazon Security Lake membuat peran IAM untuk sumber kustom pihak ketiga untuk menulis data ke data lake dan bagi pelanggan pihak ketiga untuk menggunakan data dari data lake, dan menggunakan kebijakan ini saat membuat peran ini untuk menentukan batas izin mereka.

`AmazonSecurityLakePermissionsBoundary`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSecurityLakePermissionsBoundary` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 November 2022, 14:11 UTC
- Waktu yang telah diedit: 14 Mei 2024, 20:39 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSecurityLakePermissionsBoundary`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSESFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon SES melalui AWS Management Console.

`AmazonSESFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSESFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu telah diedit: 06 Februari 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSESFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSESReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon SES melalui AWS Management Console.

`AmazonSESReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSESReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu yang telah diedit: 14 Mei 2024, 12:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSESReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSESServiceRolePolicy

Deskripsi: Memungkinkan SES mempublikasikan metrik pemantauan CloudWatch dasar Amazon atas nama sumber daya SES Anda

`AmazonSESServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan

- Waktu pembuatan: 21 Mei 2024, 16:02 UTC
- Waktu yang telah diedit: 21 Mei 2024, 16:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSESServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSNSFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon SNS melalui. AWS Management Console

`AmazonSNSFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSNSFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu telah diedit: September 24, 2024, 22:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSNSFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSNSReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon SNS melalui. AWS Management Console

`AmazonSNSReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSNSReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu telah diedit: 24 September 2024, 22:13 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSNSReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSNSRole

Deskripsi: Kebijakan default untuk peran layanan Amazon SNS.

`AmazonSNSRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSNSRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu telah diedit: 06 Februari 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSNSRole`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:PutMetricFilter",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSQSFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon SQS melalui file. AWS Management Console

`AmazonSQSFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSQSFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu telah diedit: 06 Februari 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSQSFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSQSReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon SQS melalui file. AWS Management Console

`AmazonSQSReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSQSReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu yang telah diedit: 24 Mei 2024, 18:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSQSReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      "Action" : [
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ListDeadLetterSourceQueues",
        "sqs:ListQueues",
        "sqs:ListMessageMoveTasks",
        "sqs:ListQueueTags"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSSMAutomationApproverAccess

Deskripsi: Menyediakan akses untuk melihat eksekusi otomatisasi dan mengirim keputusan persetujuan ke otomatisasi menunggu persetujuan

`AmazonSSMAutomationApproverAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSSMAutomationApproverAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 07 Agustus 2017, 23:07 UTC
- Waktu telah diedit: 07 Agustus 2017, 23:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMAutomationApproverAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSSMAutomationRole

Deskripsi: Memberikan izin untuk layanan EC2 Otomasi untuk menjalankan aktivitas yang ditentukan dalam dokumen Otomasi

`AmazonSSMAutomationRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSSMAutomationRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 05 Desember 2016, 22:09 UTC
- Waktu telah diedit: 24 Juli 2017, 23:29 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSSMAutomationRole`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:Automation*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateImage",
        "ec2:CopyImage",
```

```
        "ec2:DeregisterImage",
        "ec2:DescribeImages",
        "ec2:DeleteSnapshot",
        "ec2:StartInstances",
        "ec2:RunInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "ec2:DescribeTags",
        "cloudformation:CreateStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks",
        "cloudformation:UpdateStack",
        "cloudformation:DeleteStack"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:Automation*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSSMDirectoryServiceAccess

Deskripsi: Kebijakan ini memungkinkan Agen SSM mengakses Directory Service atas nama pelanggan untuk bergabung dengan domain instans terkelola.

`AmazonSSMDirectoryServiceAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSSMDirectoryServiceAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 15 Maret 2019, 17:44 UTC
- Waktu yang telah diedit: 15 Maret 2019, 17:44 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMDirectoryServiceAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSSMFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon SSM.

`AmazonSSMFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSSMFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 Mei 2015, 17:39 UTC
- Waktu yang telah diedit: 20 November 2019, 20:08 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMFullAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData",
        "ds:CreateComputer",
        "ds:DescribeDirectories",
        "ec2:DescribeInstanceStatus",
        "logs:*",
        "ssm:*",
        "ec2messages:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
```

```
      "Resource" : "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSSMMaintenanceWindowRole

Deskripsi: Peran Layanan yang akan digunakan untuk Jendela EC2 Pemeliharaan

`AmazonSSMMaintenanceWindowRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSSMMaintenanceWindowRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 01 Desember 2016, 15:57 UTC

- Waktu diedit: 27 Juli 2019, 00:16 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSSMMaintenanceWindowRole`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution",
        "ssm:GetParameters",
        "ssm:ListCommands",
        "ssm:SendCommand",
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:SSM*",
        "arn:aws:lambda:*:*:function:*:SSM*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "states:DescribeExecution",
        "states:StartExecution"
      ],
      "Resource" : [
        "arn:aws:states:*:*:stateMachine:SSM*",
        "arn:aws:states:*:*:execution:SSM*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:ListGroups",
        "resource-groups:ListGroupResources"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSSMManagedEC2InstanceDefaultPolicy

Deskripsi: Kebijakan ini mengaktifkan fungsionalitas AWS Systems Manager pada EC2 instans.

`AmazonSSMManagedEC2InstanceDefaultPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSSMManagedEC2InstanceDefaultPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 Agustus 2022, 20:54 UTC
- Waktu yang telah diedit: 16 Juli 2024, 18:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMManagedEC2InstanceDefaultPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSSMManagedInstanceCore

Deskripsi: Kebijakan Amazon EC2 Role untuk mengaktifkan fungsionalitas inti layanan AWS Systems Manager.

`AmazonSSMManagedInstanceCore`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSSMManagedInstanceCore` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 15 Maret 2019, 17:22 UTC
- Waktu yang telah diedit: 23 Mei 2019, 16:54 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAssociation",
        "ssm:GetDeployablePatchSnapshotForInstance",
        "ssm:GetDocument",
        "ssm:DescribeDocument",
```

```
        "ssm:GetManifest",
        "ssm:GetParameter",
        "ssm:GetParameters",
        "ssm:ListAssociations",
        "ssm:ListInstanceAssociations",
        "ssm:PutInventory",
        "ssm:PutComplianceItems",
        "ssm:PutConfigurePackageResult",
        "ssm:UpdateAssociationStatus",
        "ssm:UpdateInstanceAssociationStatus",
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2messages:AcknowledgeMessage",
        "ec2messages:DeleteMessage",
        "ec2messages:FailMessage",
        "ec2messages:GetEndpoint",
        "ec2messages:GetMessages",
        "ec2messages:SendReply"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSSMPatchAssociation

Deskripsi: Menyediakan akses ke instance turunan untuk operasi asosiasi tambalan.

`AmazonSSMPatchAssociation`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSSMPatchAssociation` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 13 Mei 2020, 16:00 UTC
- Waktu yang telah diedit: 13 Mei 2020, 16:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMPatchAssociation`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      "Effect" : "Allow",
      "Action" : "ssm:GetPatchBaseline",
      "Resource" : "arn:aws:ssm:*:*:patchbaseline/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "tag:GetResources",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:DescribePatchBaselines",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSSMReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon SSM.

`AmazonSSMReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSSMReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 Mei 2015, 17:44 UTC
- Waktu yang telah diedit: 29 Mei 2015, 17:44 UTC

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

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSSMServiceRolePolicy

Deskripsi: Menyediakan akses ke AWS Sumber Daya yang dikelola atau digunakan oleh Amazon SSM

`AmazonSSMServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 13 November 2017, 19:20 UTC
- Waktu yang telah diedit: 15 November 2024, 14:08 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSSMServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v15 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CancelCommand",
        "ssm:GetCommandInvocation",
        "ssm:ListCommandInvocations",
        "ssm:ListCommands",
        "ssm:SendCommand",
        "ssm:GetAutomationExecution",
        "ssm:GetParameters",
        "ssm:StartAutomationExecution",
        "ssm:StopAutomationExecution",
```

```
        "ssm:ListTagsForResource",
        "ssm:GetCalendarState"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/*",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:SSM*",
        "arn:aws:lambda:*:*:function:*:SSM*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "states:DescribeExecution",
        "states:StartExecution"
```

```
      ],
      "Resource" : [
        "arn:aws:states:*:*:stateMachine:SSM*",
        "arn:aws:states:*:*:execution:SSM*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:ListGroups",
        "resource-groups:ListGroupResources",
        "resource-groups:GetGroupQuery"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:SelectResourceConfig"
      ],
      "Resource" : [
        "*"
      ]
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "compute-optimizer:GetEC2InstanceRecommendations",
        "compute-optimizer:GetEnrollmentStatus"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "support:DescribeTrustedAdvisorChecks",
        "support:DescribeTrustedAdvisorCheckSummaries",
        "support:DescribeTrustedAdvisorCheckResult",
        "support:DescribeCases"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeComplianceByConfigRule",
        "config:DescribeComplianceByResource",
        "config:DescribeRemediationConfigurations",
        "config:DescribeConfigurationRecorders"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:DescribeAlarms",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "organizations:DescribeOrganization",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudformation:ListStackSets",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStackInstances",
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:DeleteStackSet"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stackset/AWS-QuickSetup-SSM*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudformation:DeleteStackInstances",
      "Resource" : [
        "arn:aws:cloudformation:*:*:stackset/AWS-QuickSetup-SSM*:*",
        "arn:aws:cloudformation:*:*:stackset-target/AWS-QuickSetup-SSM*:*",
        "arn:aws:cloudformation:*:*:type/resource/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "events:ManagedBy" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:RemoveTargets",
        "events:DeleteRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/SSMExplorerManagedRule"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "events:DescribeRule",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "securityhub:DescribeHub",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "resource-explorer-2:CreateManagedView",
      "Resource" : "arn:aws:resource-explorer-2:*:*:managed-view/AWSManagedViewForSSM*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSumerianFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Sumeria.

`AmazonSumerianFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSumerianFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 24 April 2018, 20:14 UTC
- Waktu yang telah diedit: 24 April 2018, 20:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSumerianFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonTextractFullAccess

Deskripsi: Akses ke semua Amazon Textract APIs

`AmazonTextractFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonTextractFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 November 2018, 19:07 UTC
- Waktu telah diedit: 28 November 2018, 19:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTextractFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonTextractServiceRole

Deskripsi: Memungkinkan Textract untuk memanggil AWS layanan atas nama Anda.

`AmazonTextractServiceRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonTextractServiceRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 28 November 2018, 19:12 UTC
- Waktu telah diedit: 28 November 2018, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonTextractServiceRole`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonTimestreamConsoleFullAccess

Deskripsi: Menyediakan akses penuh untuk mengelola Amazon Timestream menggunakan file. AWS Management Console Perhatikan bahwa kebijakan ini juga memberikan izin untuk operasi KMS tertentu, dan operasi untuk mengelola kueri yang disimpan. Jika menggunakan CMK yang dikelola Pelanggan, silakan merujuk ke dokumentasi untuk izin tambahan yang diperlukan.

`AmazonTimestreamConsoleFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonTimestreamConsoleFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 30 September 2020, 21:47 UTC
- Waktu telah diedit: 17 Juni 2025, 13:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamConsoleFullAccess`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "timestream:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListKeys",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : [
        "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" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonTimestreamFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Timestream. Perhatikan bahwa kebijakan ini juga memberikan akses operasi KMS tertentu. Jika menggunakan CMK yang dikelola Pelanggan, silakan merujuk ke dokumentasi untuk izin tambahan yang diperlukan.

`AmazonTimestreamFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonTimestreamFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 September 2020, 21:47 UTC
- Waktu yang telah diedit: 26 November 2021, 23:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "timestream:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:timestream:database-name"
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        },
        "StringLike" : {
          "kms:ViaService" : "timestream.*.amazonaws.com"
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonTimestreamInfluxDBFullAccess

Deskripsi: Menyediakan akses administratif penuh untuk membuat, memperbarui, menghapus, dan mencantumkan instans Amazon TimeStream InfluxDB serta membuat serta mencantumkan grup parameter. Silakan merujuk ke dokumentasi untuk izin tambahan yang diperlukan.

`AmazonTimestreamInfluxDBFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonTimestreamInfluxDBFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 14 Maret 2024, 22:53 UTC
- Waktu telah diedit: 17 April 2025, 18:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamInfluxDBFullAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TimestreamInfluxDBStatement",
      "Effect" : "Allow",
      "Action" : [
        "timestream-influxdb:CreateDbParameterGroup",
        "timestream-influxdb:GetDbParameterGroup",
        "timestream-influxdb:ListDbParameterGroups",
        "timestream-influxdb:CreateDbInstance",
        "timestream-influxdb:DeleteDbInstance",
        "timestream-influxdb:GetDbInstance",
        "timestream-influxdb:ListDbInstances",
        "timestream-influxdb:TagResource",
        "timestream-influxdb:UntagResource",
        "timestream-influxdb:ListTagsForResource",
        "timestream-influxdb:UpdateDbInstance",
        "timestream-influxdb:CreateDbCluster",
        "timestream-influxdb:GetDbCluster",
        "timestream-influxdb:UpdateDbCluster",
        "timestream-influxdb:DeleteDbCluster",
        "timestream-influxdb:ListDbClusters",
        "timestream-influxdb:ListDbInstancesForCluster"
      ],
      "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"
      ],
      "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"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonTimestreamInfluxDBFullAccessWithoutMarketplaceAccess

Deskripsi: Menyediakan akses administratif untuk mengelola instans Amazon TimeStream InfluxDB dan grup parameter kecuali operasi marketplace.

`AmazonTimestreamInfluxDBFullAccessWithoutMarketplaceAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonTimestreamInfluxDBFullAccessWithoutMarketplaceAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 17 April 2025, 17:52 UTC
- Waktu yang telah diedit: 17 April 2025, 17:52 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamInfluxDBFullAccessWithoutMarketplaceAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
        "timestream-influxdb:CreateDbParameterGroup",
        "timestream-influxdb:GetDbParameterGroup",
        "timestream-influxdb:ListDbParameterGroups",
        "timestream-influxdb:CreateDbInstance",
        "timestream-influxdb:DeleteDbInstance",
        "timestream-influxdb:GetDbInstance",
        "timestream-influxdb:ListDbInstances",
        "timestream-influxdb:TagResource",
        "timestream-influxdb:UntagResource",
        "timestream-influxdb:ListTagsForResource",
        "timestream-influxdb:UpdateDbInstance",
        "timestream-influxdb:CreateDbCluster",
        "timestream-influxdb:GetDbCluster",
        "timestream-influxdb:UpdateDbCluster",
        "timestream-influxdb:DeleteDbCluster",
        "timestream-influxdb:ListDbClusters",
        "timestream-influxdb:ListDbInstancesForCluster"
      ],
      "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"
      ],
      "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:::*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonTimestreamInfluxDBServiceRolePolicy

Deskripsi: Menyediakan akses administratif penuh untuk membuat, memperbarui, menghapus, dan mencantumkan instans Amazon TimeStream InfluxDB serta membuat serta mencantumkan grup parameter. Silakan merujuk ke dokumentasi untuk izin tambahan yang diperlukan.

`AmazonTimestreamInfluxDBServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 14 Maret 2024, 18:53 UTC
- Waktu yang telah diedit: 14 Maret 2024, 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonTimestreamInfluxDBServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateEniInSubnetStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "CreateEniStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AmazonTimestreamInfluxDBManaged" : "false"
        }
      }
    },
    {
      "Sid" : "CreateTagWithEniStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AmazonTimestreamInfluxDBManaged" : "false"
        },
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateNetworkInterface"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "ManageEniStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonTimestreamInfluxDBManaged" : "false"
        }
      }
    },
    {
      "Sid" : "PutCloudWatchMetricsStatement",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/Timestream/InfluxDB",
            "AWS/Usage"
          ]
        }
      },
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ManageSecretStatement",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret"
      ],
      "Resource" : [
```

```
        "arn:aws:secretsmanager:*:*:secret:READONLY-InfluxDB-auth-parameters-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonTimestreamReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon Timestream. Kebijakan juga memberikan izin untuk membatalkan kueri yang sedang berjalan. Jika menggunakan CMK yang dikelola Pelanggan, silakan merujuk ke dokumentasi untuk izin tambahan yang diperlukan.

`AmazonTimestreamReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonTimestreamReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 September 2020, 21:47 UTC
- Waktu telah diedit: 05 Juni 2024, 19:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonTranscribeFullAccess

Deskripsi: Menyediakan akses penuh ke operasi Amazon Transcribe

`AmazonTranscribeFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonTranscribeFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 04 April 2018, 16:06 UTC
- Waktu yang telah diedit: 04 April 2018, 16:06 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTranscribeFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*transcribe*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonTranscribeReadOnlyAccess

Deskripsi: Menyediakan akses ke operasi baca saja untuk Amazon Transcribe

`AmazonTranscribeReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonTranscribeReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 04 April 2018, 16:05 UTC
- Waktu yang telah diedit: 04 April 2018, 16:05 UTC

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

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonVerifiedPermissionsFullAccess

Deskripsi: Menyediakan akses penuh ke Izin Terverifikasi

`AmazonVerifiedPermissionsFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonVerifiedPermissionsFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 11 Oktober 2024, 18:19 UTC
- Waktu yang telah diedit: 11 Oktober 2024, 18:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVerifiedPermissionsFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonVerifiedPermissionsReadOnlyAccess

Deskripsi: Menyediakan akses hanya-baca ke layanan Izin Terverifikasi.

`AmazonVerifiedPermissionsReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonVerifiedPermissionsReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 11 Oktober 2024, 18:25 UTC
- Waktu yang telah diedit: 11 Oktober 2024, 18:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVerifiedPermissionsReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonVPCCrossAccountNetworkInterfaceOperations

Deskripsi: Menyediakan akses untuk membuat antarmuka jaringan dan melampirkannya ke sumber daya lintas akun

`AmazonVPCCrossAccountNetworkInterfaceOperations`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonVPCCrossAccountNetworkInterfaceOperations` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 Juli 2017, 20:47 UTC
- Waktu yang telah diedit: September 25, 2023, 15:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCCrossAccountNetworkInterfaceOperations`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeRouteTables",
        "ec2:CreateRoute",
        "ec2:DeleteRoute",
        "ec2:ReplaceRoute"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeRegions",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:AssignIpv6Addresses",
        "ec2:UnassignIpv6Addresses"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonVPCFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon VPC melalui file. AWS Management Console

`AmazonVPCFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonVPCFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu telah diedit: 09 Desember 2024, 17:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCFullAccess`

Versi kebijakan

Versi kebijakan: v11 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonVPCFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AcceptVpcPeeringConnection",
        "ec2:AcceptVpcEndpointConnections",
        "ec2:AllocateAddress",
        "ec2:AssignIpv6Addresses",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssociateAddress",
        "ec2:AssociateDhcpOptions",
        "ec2:AssociateRouteTable",
        "ec2: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" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonVPCNetworkAccessAnalyzerFullAccessPolicy

Deskripsi: Menyediakan izin untuk mendeskripsikan AWS sumber daya, menjalankan Network Access Analyzer, dan membuat atau menghapus tag pada Network Insights Access Scope dan Network Insights Access Scope Analysis.

`AmazonVPCNetworkAccessAnalyzerFullAccessPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonVPCNetworkAccessAnalyzerFullAccessPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 15 Juni 2023, 22:56 UTC
- Waktu yang telah diedit: 15 Mei 2024, 21:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCNetworkAccessAnalyzerFullAccessPolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonVPCReachabilityAnalyzerFullAccessPolicy

Deskripsi: Memberikan izin untuk mendeskripsikan AWS sumber daya, menjalankan Reachability Analyzer, dan membuat atau menghapus tag di Jalur Wawasan Jaringan dan Analisis Wawasan Jaringan.

`AmazonVPCReachabilityAnalyzerFullAccessPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonVPCReachabilityAnalyzerFullAccessPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 14 Juni 2023, 20:12 UTC
- Waktu yang telah diedit: 15 Mei 2024, 20:47 UTC

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

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonVPCReachabilityAnalyzerPathComponentReadPolicy

Deskripsi: Kebijakan ini dilampirkan pada peran IAMRoleForReachabilityAnalyzerCrossAccountResourceAccess. Peran ini diterapkan ke akun anggota di organisasi saat akun manajemen mengaktifkan akses tepercaya untuk Reachability Analyzer. Ini memberikan izin untuk melihat sumber daya dari seluruh organisasi Anda menggunakan konsol Reachability Analyzer.

`AmazonVPCReachabilityAnalyzerPathComponentReadPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonVPCReachabilityAnalyzerPathComponentReadPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Mei 2023, 20:38 UTC
- Waktu yang telah diedit: 01 Mei 2023, 20:38 UTC

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

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonVPCReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon VPC melalui file. AWS Management Console

`AmazonVPCReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonVPCReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu yang telah diedit: 09 Desember 2024, 15:06 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v10 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonVPCReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeCarrierGateways",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLocalGatewayRouteTables",
```

```
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeMovingAddresses",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupReferences",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
        "ec2: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" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonWorkDocsFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon WorkDocs melalui AWS Management Console

`AmazonWorkDocsFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonWorkDocsFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 16 April 2020, 23:05 UTC
- Waktu yang telah diedit: 16 April 2020, 23:05 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkDocsFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "workdocs:*",
        "ds:DescribeDirectories",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
```

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonWorkDocsReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon WorkDocs melalui AWS Management Console

`AmazonWorkDocsReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonWorkDocsReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 08 Januari 2020, 23:49 UTC
- Waktu yang telah diedit: 08 Januari 2020, 23:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkDocsReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "workdocs:Describe*",
        "ds:DescribeDirectories",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonWorkMailEventsServiceRolePolicy

Deskripsi: Mengaktifkan akses ke Layanan AWS dan Sumber Daya yang digunakan atau dikelola oleh Amazon WorkMail Events

`AmazonWorkMailEventsServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 16 April 2019, 16:52 UTC
- Waktu yang telah diedit: 16 April 2019, 16:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonWorkMailEventsServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonWorkMailFullAccess

Deskripsi: Menyediakan akses penuh ke WorkMail, Directory Service, SES, EC2 dan akses baca ke metadata KMS.

`AmazonWorkMailFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonWorkMailFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu yang telah diedit: 21 Desember 2020, 14:13 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkMailFullAccess`

Versi kebijakan

Versi kebijakan: v10 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ds:AuthorizeApplication",
        "ds:CheckAlias",
        "ds:CreateAlias",
        "ds:CreateDirectory",
        "ds:CreateIdentityPoolDirectory",
        "ds:DeleteDirectory",
```

```
        "ds:DescribeDirectories",
        "ds:GetDirectoryLimits",
        "ds:ListAuthorizedApplications",
        "ds:UnauthorizeApplication",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateTags",
        "ec2:CreateVpc",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteSubnet",
        "ec2:DeleteVpc",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "kms:DescribeKey",
        "kms:ListAliases",
        "lambda:ListFunctions",
        "route53:ChangeResourceRecordSets",
        "route53:ListHostedZones",
        "route53:ListResourceRecordSets",
        "route53:GetHostedZone",
        "route53domains:CheckDomainAvailability",
        "route53domains:ListDomains",
        "ses:*",
        "workmail:*",
        "iam:ListRoles",
        "logs:DescribeLogGroups",
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy",
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "iam:AWSServiceName" : "events.workmail.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/events.workmail.amazonaws.com/
AWSServiceRoleForAmazonWorkMailEvents*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*workmail*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "events.workmail.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonWorkMailMessageFlowFullAccess

Deskripsi: Akses penuh ke Alur WorkMail Pesan APIs

`AmazonWorkMailMessageFlowFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonWorkMailMessageFlowFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 11 Februari 2021 11:08 UTC
- Waktu yang telah diedit: 11 Februari 2021, 11:08 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkMailMessageFlowFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonWorkMailMessageFlowReadOnlyAccess

Deskripsi: Akses hanya membaca ke WorkMail pesan untuk GetRawMessageContent API

`AmazonWorkMailMessageFlowReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonWorkMailMessageFlowReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 Januari 2021, 12:40 UTC
- Waktu yang telah diedit: 28 Januari 2021, 12:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkMailMessageFlowReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      "Action" : [
        "workmailmessageflow:Get*"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonWorkMailReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke WorkMail dan SES.

`AmazonWorkMailReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonWorkMailReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu yang telah diedit: 25 Juli 2019, 08:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkMailReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ses:Describe*",
        "ses:Get*",
        "workmail:Describe*",
        "workmail:Get*",
        "workmail:List*",
        "workmail:Search*",
        "lambda:ListFunctions",
        "iam:ListRoles",
        "logs:DescribeLogGroups",
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonWorkSpacesAdmin

Deskripsi: Menyediakan akses ke tindakan WorkSpaces administratif Amazon melalui AWS SDK dan CLI.

`AmazonWorkSpacesAdmin`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonWorkSpacesAdmin` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 22 September 2015, 22:21 UTC
- Waktu yang telah diedit: 27 Juni 2024, 17:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesAdmin`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonWorkSpacesApplicationManagerAdminAccess

Deskripsi: Menyediakan akses administrator untuk mengemas aplikasi di Amazon WorkSpaces Application Manager.

`AmazonWorkSpacesApplicationManagerAdminAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonWorkSpacesApplicationManagerAdminAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 09 April 2015, 14:03 UTC
- Waktu yang telah diedit: 09 April 2015, 14:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesApplicationManagerAdminAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonWorkspacesPCAAccess

Deskripsi: Kebijakan terkelola ini menyediakan akses administratif penuh ke sumber daya AWS Certificate Manager Private CA Akun AWS untuk autentikasi berbasis sertifikat.

`AmazonWorkspacesPCAAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonWorkspacesPCAAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 08 November 2022, 00:25 UTC
- Waktu yang telah diedit: 08 November 2022, 00:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkspacesPCAAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonWorkSpacesPoolServiceAccess

Deskripsi: Kebijakan ini menyediakan akses AWS WorkSpaces layanan ke sumber daya akun pelanggan yang diperlukan untuk meluncurkan Workspaces Pools

`AmazonWorkSpacesPoolServiceAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonWorkSpacesPoolServiceAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Juni 2024, 16:21 UTC
- Waktu telah diedit: 27 Juni 2024, 16:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesPoolServiceAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonWorkSpacesSecureBrowserReadOnly

Deskripsi: Menyediakan akses hanya-baca ke Amazon WorkSpaces Secure Browser dan dependensinya melalui, SDK AWS Management Console, dan CLI.

`AmazonWorkSpacesSecureBrowserReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonWorkSpacesSecureBrowserReadOnly` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 24 Juni 2024, 20:01 UTC
- Waktu yang telah diedit: 24 Juni 2024, 20:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesSecureBrowserReadOnly`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonWorkSpacesSelfServiceAccess

Deskripsi: Menyediakan akses ke layanan WorkSpaces backend Amazon untuk melakukan tindakan Layanan Mandiri Workspace

`AmazonWorkSpacesSelfServiceAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonWorkSpacesSelfServiceAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Juni 2019, 19:22 UTC
- Waktu yang telah diedit: 27 Juni 2019, 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesSelfServiceAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "workspaces:RebootWorkspaces",
        "workspaces:RebuildWorkspaces",
        "workspaces:ModifyWorkspaceProperties"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonWorkSpacesServiceAccess

Deskripsi: Menyediakan akses akun pelanggan ke AWS WorkSpaces layanan untuk meluncurkan Workspace.

`AmazonWorkSpacesServiceAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonWorkSpacesServiceAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Juni 2019, 19:19 UTC
- Waktu diedit: 18 Maret 2020, 23:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesServiceAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonWorkSpacesThinClientFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon WorkSpaces Thin Client serta akses terbatas ke layanan terkait yang diperlukan

`AmazonWorkSpacesThinClientFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonWorkSpacesThinClientFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 09 Agustus 2024, 07:25 UTC
- Waktu telah diedit: 09 Januari 2025, 16:52 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesThinClientFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonWorkSpacesThinClientMonitoringServiceRolePolicy

Deskripsi: Mengaktifkan akses ke Layanan AWS dan Sumber Daya yang digunakan atau dikelola oleh Amazon WorkSpaces Thin Client Monitoring

`AmazonWorkSpacesThinClientMonitoringServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 13 Juni 2025, 19:37 UTC

- Waktu telah diedit: 13 Juni 2025, 19:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonWorkSpacesThinClientMonitoringServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonWorkSpacesThinClientReadOnlyAccess

Deskripsi: Menyediakan akses hanya-baca ke Amazon WorkSpaces Thin Client dan dependensinya

`AmazonWorkSpacesThinClientReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonWorkSpacesThinClientReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 19 Juli 2024, 08:50 UTC
- Waktu telah diedit: 09 Januari 2025, 16:52 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesThinClientReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonWorkSpacesWebReadOnly

Deskripsi: Menyediakan akses hanya-baca ke Amazon WorkSpaces Web dan dependensinya melalui, SDK AWS Management Console, dan CLI.

`AmazonWorkSpacesWebReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonWorkSpacesWebReadOnly` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 November 2021 14:20 UTC
- Waktu telah diedit: 02 November 2022, 20.20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesWebReadOnly`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      "Action" : [
        "workspaces-web:GetBrowserSettings",
        "workspaces-web:GetIdentityProvider",
        "workspaces-web:GetNetworkSettings",
        "workspaces-web:GetPortal",
        "workspaces-web:GetPortalServiceProviderMetadata",
        "workspaces-web:GetTrustStore",
        "workspaces-web:GetTrustStoreCertificate",
        "workspaces-web:GetUserSettings",
        "workspaces-web:GetUserAccessLoggingSettings",
        "workspaces-web:ListBrowserSettings",
        "workspaces-web:ListIdentityProviders",
        "workspaces-web:ListNetworkSettings",
        "workspaces-web:ListPortals",
        "workspaces-web:ListTagsForResource",
        "workspaces-web:ListTrustStoreCertificates",
        "workspaces-web:ListTrustStores",
        "workspaces-web:ListUserSettings",
        "workspaces-web:ListUserAccessLoggingSettings"
      ],
      "Resource" : "arn:aws:workspaces-web:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "kinesis:ListStreams"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonWorkSpacesWebServiceRolePolicy

Deskripsi: Mengaktifkan akses ke Layanan AWS dan Sumber Daya yang digunakan atau dikelola oleh Amazon WorkSpaces Web

`AmazonWorkSpacesWebServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 30 November 2021, 13:15 UTC
- Waktu telah diedit: 15 Desember 2022, 22.46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonWorkSpacesWebServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonZocaloFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Zocalo.

`AmazonZocaloFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonZocaloFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu telah diedit: 06 Februari 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonZocaloFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      "Action" : [
        "zocalo:*",
        "ds:*",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateTags",
        "ec2:CreateVpc",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonZocaloReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon Zocalo

`AmazonZocaloReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonZocaloReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu telah diedit: 06 Februari 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonZocaloReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "zocalo:Describe*",
        "ds:DescribeDirectories",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmplifyBackendDeployFullAccess

Deskripsi: Menyediakan izin akses penuh Amplify untuk menerapkan sumber daya backend Amplify (, Amazon AWS AppSync Cognito, Amazon S3, dan layanan terkait lainnya) melalui Kit Pengembangan (CDK) AWS Cloud AWS

`AmplifyBackendDeployFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmplifyBackendDeployFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 06 Oktober 2023, 21:32 UTC
- Waktu telah diedit: 14 November 2024, 19:09 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmplifyBackendDeployFullAccess`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

APIGatewayServiceRolePolicy

Deskripsi: Memungkinkan API Gateway mengelola AWS Sumber Daya terkait atas nama pelanggan.

`APIGatewayServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 20 Oktober 2017, 17:23 UTC
- Waktu yang telah diedit: 12 Juli 2021 22:24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/APIGatewayServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddListenerCertificates",
        "elasticloadbalancing:RemoveListenerCertificates",
        "elasticloadbalancing:ModifyListener",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancers",
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingTargets",
        "xray:GetSamplingRules",
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries",
        "servicediscovery:DiscoverInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:DescribeDeliveryStream",
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : "arn:aws:firehose:*:*:deliverystream/amazon-apigateway-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate",
        "acm:GetCertificate"
      ],
```

```
      "Resource" : "arn:aws:acm:*:*:certificate/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterfacePermission",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Owner",
            "VpcLinkId"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface",
        "ec2:AssignPrivateIpAddresses",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:UnassignPrivateIpAddresses",
        "ec2:DescribeSubnets",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "servicediscovery:GetNamespace",
      "Resource" : "arn:aws:servicediscovery:*:*:namespace/*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : "servicediscovery:GetService",
      "Resource" : "arn:aws:servicediscovery:*:*:service/*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AppIntegrationsServiceLinkedRolePolicy

Deskripsi: Memungkinkan AppIntegrations untuk mengelola AppFlow sumber daya dan mempublikasikan data CloudWatch metrik atas nama Anda.

`AppIntegrationsServiceLinkedRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 30 September 2022, 19.42 UTC
- Waktu yang telah diedit: 30 September 2022 19.42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AppIntegrationsServiceLinkedRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

ApplicationAutoScalingForAmazonAppStreamAccess

Deskripsi: Kebijakan untuk mengaktifkan Penskalaan Otomatis Aplikasi untuk Amazon AppStream

`ApplicationAutoScalingForAmazonAppStreamAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ApplicationAutoScalingForAmazonAppStreamAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 06 Februari 2017, 21:39 UTC
- Waktu telah diedit: 06 Februari 2017, 21:39 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ApplicationAutoScalingForAmazonAppStreamAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

ApplicationDiscoveryServiceContinuousExportServiceRolePolicy

Deskripsi: Mengaktifkan akses ke Layanan AWS dan Sumber Daya yang digunakan atau dikelola oleh fitur Ekspor Berkelanjutan Application Discovery Service

`ApplicationDiscoveryServiceContinuousExportServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 09 Agustus 2018, 20:22 UTC
- Waktu telah diedit: 13 Agustus 2018, 22:31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ApplicationDiscoveryServiceContinuousExportServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "glue:CreateDatabase",
        "glue:UpdateDatabase",
        "glue:CreateTable",
        "glue:UpdateTable",
        "firehose:CreateDeliveryStream",
        "firehose:DescribeDeliveryStream",
        "logs:CreateLogGroup"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "firehose:DeleteDeliveryStream",
        "firehose:PutRecord",
        "firehose:PutRecordBatch",
        "firehose:UpdateDestination"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:firehose:*:*:deliverystream/aws-application-discovery-
service*"
    },
    {
      "Action" : [
        "s3:CreateBucket",
        "s3:ListBucket",
        "s3:PutBucketLogging",
        "s3:PutEncryptionConfiguration"
```

```
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:s3:::aws-application-discovery-service*"
    },
    {
      "Action" : [
        "s3:GetObject"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:s3:::aws-application-discovery-service*/*"
    },
    {
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutRetentionPolicy"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/application-discovery-service/
firehose*"
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/AWSApplicationDiscoveryServiceFirehose",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "firehose.amazonaws.com"
        }
      }
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/service-role/
AWSApplicationDiscoveryServiceFirehose",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "firehose.amazonaws.com"
        }
      }
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AppRunnerNetworkingServiceRolePolicy

Deskripsi: Memungkinkan AWS AppRunner Jaringan untuk mengelola AWS sumber daya terkait atas nama Anda.

`AppRunnerNetworkingServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 12 Januari 2022, 21:02 UTC
- Waktu yang telah diedit: 12 Januari 2022, 21.02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AppRunnerNetworkingServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AWSAppRunnerManaged"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        },
        "StringLike" : {
          "aws:RequestTag/AWSAppRunnerManaged" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : "ec2:DeleteNetworkInterface",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSAppRunnerManaged" : "false"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AppRunnerServiceRolePolicy

Deskripsi: Memungkinkan AWS AppRunner untuk mengelola AWS sumber daya terkait atas nama Anda.

`AppRunnerServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 14 Mei 2021 19:15 UTC
- Waktu yang telah diedit: 14 Mei 2021 19.15 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AppRunnerServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/apprunner/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/apprunner/*:log-stream:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:DescribeRule",
        "events:EnableRule",
        "events:DisableRule"
      ],
```

```
      "Resource" : "arn:aws:events:*:*:rule/AWSAppRunnerManagedRule*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AppStudioServiceRolePolicy

Deskripsi: Memungkinkan AppStudio untuk mengelola AWS sumber daya terkait atas nama Anda.

`AppStudioServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 10 Juli 2024, 05:01 UTC
- Waktu telah diedit: 13 Maret 2025, 20:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AppStudioServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AuroraDsqlServiceLinkedRolePolicy

Deskripsi: Kebijakan untuk Peran Tertaut Layanan Amazon Aurora DSQL

`AuroraDsqlServiceLinkedRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 03 Desember 2024, 15:06 UTC
- Waktu yang telah diedit: 09 Mei 2025, 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AuroraDsqlServiceLinkedRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/AuroraDSQL",
            "AWS/Usage"
          ],
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AutoScalingConsoleFullAccess

Deskripsi: Menyediakan akses penuh ke Auto Scaling melalui. AWS Management Console

`AutoScalingConsoleFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AutoScalingConsoleFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 12 Januari 2017, 19:43 UTC
- Waktu telah diedit: 06 Februari 2018, 23:15 UTC
- ARN: `arn:aws:iam::aws:policy/AutoScalingConsoleFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateKeyPair",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSpotInstanceRequests",
```

```
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcClassicLink",
        "ec2:ImportKeyPair"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:Describe*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "autoscaling:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:ListSubscriptions",
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:ListRoles",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "autoscaling.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AutoScalingConsoleReadOnlyAccess

Deskripsi: Menyediakan akses hanya-baca ke Auto Scaling melalui. AWS Management Console

`AutoScalingConsoleReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AutoScalingConsoleReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 12 Januari 2017, 19:48 UTC
- Waktu telah diedit: 12 Januari 2017, 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/AutoScalingConsoleReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:Describe*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "autoscaling:Describe*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:ListSubscriptions",
        "sns:ListTopics"
```

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AutoScalingFullAccess

Deskripsi: Menyediakan akses penuh ke Auto Scaling.

`AutoScalingFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AutoScalingFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 12 Januari 2017, 19:31 UTC
- Waktu telah diedit: 06 Februari 2018, 21:59 UTC
- ARN: `arn:aws:iam::aws:policy/AutoScalingFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "autoscaling:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricAlarm",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcClassicLink"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "autoscaling.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AutoScalingNotificationAccessRole

Deskripsi: Kebijakan default untuk peran layanan Akses AutoScaling Pemberitahuan.

`AutoScalingNotificationAccessRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AutoScalingNotificationAccessRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu telah diedit: 06 Februari 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AutoScalingNotificationAccessRole`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "sqs:SendMessage",
        "sqs:GetQueueUrl",
        "sns:Publish"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AutoScalingReadOnlyAccess

Deskripsi: Menyediakan akses read-only ke Auto Scaling.

`AutoScalingReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AutoScalingReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 12 Januari 2017, 19:39 UTC
- Waktu telah diedit: 12 Januari 2017, 19:39 UTC
- ARN: `arn:aws:iam::aws:policy/AutoScalingReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AutoScalingServiceRolePolicy

Deskripsi: Mengaktifkan akses ke Layanan AWS dan Sumber Daya yang digunakan atau dikelola oleh Auto Scaling

`AutoScalingServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 08 Januari 2018, 23:10 UTC
- Waktu telah diedit: November 15, 2024, 17:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AutoScalingServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2InstanceManagement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachClassicLinkVpc",
```

```
        "ec2:CancelSpotInstanceRequests",
        "ec2:CreateFleet",
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "ec2:Describe*",
        "ec2:DetachClassicLinkVpc",
        "ec2:GetInstanceTypesFromInstanceRequirements",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:ModifyInstanceAttribute",
        "ec2:RequestSpotInstances",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2InstanceProfileManagement",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.amazonaws.com*"
        }
      }
    },
    {
      "Sid" : "EC2SpotManagement",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "spot.amazonaws.com"
        }
      }
    },
    {
```

```
      "Sid" : "ELBManagement",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:Register*",
        "elasticloadbalancing:Deregister*",
        "elasticloadbalancing:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CWManagement",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SNSManagement",
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EventBridgeRuleManagement",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets",
        "events:DeleteRule",
        "events:DescribeRule"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "autoscaling.amazonaws.com"
        }
      }
```

```
    },
    {
      "Sid" : "SystemsManagerParameterManagement",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameters"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VpcLatticeManagement",
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:DeregisterTargets",
        "vpc-lattice:GetTargetGroup",
        "vpc-lattice:ListTargets",
        "vpc-lattice:ListTargetGroups",
        "vpc-lattice:RegisterTargets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ResourceGroupsManagement",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:ListGroupResources"
      ],
      "Resource" : "arn:*:resource-groups:*:*:group/*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWS-SSM-Automation-DiagnosisBucketPolicy

Deskripsi: Memberikan izin untuk mengakses bucket SSM Diagnosis S3 untuk diagnosis dan remediasi masalah.

`AWS-SSM-Automation-DiagnosisBucketPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWS-SSM-Automation-DiagnosisBucketPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 15 November 2024, 23:31 UTC
- Waktu telah diedit: 15 November 2024, 23:31 UTC
- ARN: `arn:aws:iam::aws:policy/AWS-SSM-Automation-DiagnosisBucketPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy

Deskripsi: Memberikan izin untuk Mendiagnosis masalah dengan layanan SSM dengan menjalankan aktivitas yang ditentukan dalam Dokumen Otomasi, terutama digunakan untuk menjalankan dokumen Otomasi dalam pengaturan lintas wilayah lintas akun dengan memicu otomatisasi anak dalam akun anggota.

`AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 16 November 2024, 00:01 UTC
- Waktu yang telah diedit: 16 November 2024, 00:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy

Deskripsi: Memberikan izin untuk Mendiagnosis masalah dengan layanan SSM dengan menjalankan aktivitas yang ditentukan dalam Dokumen Otomasi, terutama digunakan untuk menjalankan dokumen Otomasi dalam pengaturan akun/wilayah target dengan mendiagnosis kesehatan layanan SSM di semua node.

`AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 16 November 2024, 00:08 UTC
- Waktu telah diedit: 16 November 2024, 00:08 UTC
- ARN: `arn:aws:iam::aws:policy/AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrationRolePolicy

Deskripsi: Memberikan izin untuk akun operasional untuk mendiagnosis node yang tidak dikelola dengan memberikan izin khusus Organisasi yang diperlukan oleh otomatisasi SSM untuk menarik daftar akun anggota dalam akar Organisasi untuk memicu eksekusi lintas wilayah lintas akun dengan mengizinkan asumsi peran Eksekusi di akun/wilayah target.

`AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrationRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrationRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 16 November 2024, 00:11 UTC
- Waktu yang telah diedit: 16 November 2024, 00:11 UTC
- ARN: `arn:aws:iam::aws:policy/AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrationRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWS-SSM-RemediationAutomation-AdministrationRolePolicy

Deskripsi: Memberikan izin untuk memulihkan masalah dengan layanan SSM dengan menjalankan aktivitas yang ditentukan dalam Dokumen Otomasi, terutama digunakan untuk menjalankan dokumen Otomasi dalam pengaturan lintas wilayah lintas akun dengan memicu otomatisasi anak dalam akun anggota.

`AWS-SSM-RemediationAutomation-AdministrationRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWS-SSM-RemediationAutomation-AdministrationRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 16 November 2024, 00:14 UTC
- Waktu yang telah diedit: 16 November 2024, 00:14 UTC
- ARN: `arn:aws:iam::aws:policy/AWS-SSM-RemediationAutomation-AdministrationRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWS-SSM-RemediationAutomation-ExecutionRolePolicy

Deskripsi: Memberikan izin untuk Memperbaiki masalah dengan layanan SSM dengan menjalankan aktivitas yang ditentukan dalam Dokumen Otomasi, terutama digunakan untuk menjalankan dokumen Otomasi dalam pengaturan akun/wilayah target dengan memulihkan kesehatan layanan SSM di semua node.

`AWS-SSM-RemediationAutomation-ExecutionRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWS-SSM-RemediationAutomation-ExecutionRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 16 November 2024, 00:17 UTC
- Waktu yang telah diedit: 16 November 2024, 00:17 UTC
- ARN: `arn:aws:iam::aws:policy/AWS-SSM-RemediationAutomation-ExecutionRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWS-SSM-RemediationAutomation-OperationalAccountAdministrationRolePolicy

Deskripsi: Memberikan izin untuk akun operasional untuk Memulihkan node yang tidak dikelola dengan memberikan izin khusus Organisasi yang diperlukan oleh otomatisasi SSM untuk menarik daftar akun anggota dalam akar Organisasi untuk memicu eksekusi lintas wilayah lintas akun dengan mengizinkan asumsi peran Eksekusi di akun/wilayah target.

`AWS-SSM-RemediationAutomation-OperationalAccountAdministrationRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWS-SSM-RemediationAutomation-OperationalAccountAdministrationRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 16 November 2024, 00:25 UTC
- Waktu yang telah diedit: 16 November 2024, 00:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWS-SSM-RemediationAutomation-OperationalAccountAdministrationRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWS_ConfigRole

Deskripsi: Kebijakan default untuk peran layanan AWS Config. Menyediakan izin yang diperlukan untuk AWS Config untuk melacak perubahan pada sumber daya Anda AWS .

`AWS_ConfigRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWS_ConfigRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 15 September 2020, 20:30 UTC
- Waktu yang telah diedit: 20 Juni 2025, 17:22 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWS_ConfigRole`

Versi kebijakan

Versi kebijakan: v38 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
  "Statement" : [
    {
      "Sid" : "AWSConfigRoleStatementID",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:GetAnalyzer",
        "access-analyzer:GetArchiveRule",
        "access-analyzer:ListAnalyzers",
        "access-analyzer:ListArchiveRules",
        "access-analyzer:ListTagsForResource",
        "account:GetAlternateContact",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:GetCertificateAuthorityCsr",
        "acm-pca:ListCertificateAuthorities",
        "acm-pca:ListTags",
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "acm:ListTagsForCertificate",
        "airflow:GetEnvironment",
        "airflow:ListEnvironments",
        "airflow:ListTagsForResource",
        "amplify:GetApp",
        "amplify:GetBranch",
        "amplify:ListApps",
        "amplify:ListBranches",
        "amplifyuibuilder:ExportThemes",
        "amplifyuibuilder:GetTheme",
        "amplifyuibuilder:ListThemes",
        "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:GetEventIntegration",
```

```
        "app-integrations:ListApplications",
        "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",
        "appmesh:DescribeGatewayRoute",
        "appmesh:DescribeMesh",
        "appmesh:DescribeRoute",
        "appmesh:DescribeVirtualGateway",
        "appmesh:DescribeVirtualNode",
        "appmesh:DescribeVirtualRouter",
        "appmesh:DescribeVirtualService",
        "appmesh:ListGatewayRoutes",
        "appmesh:ListMeshes",
        "appmesh:ListRoutes",
        "appmesh:ListTagsForResource",
        "appmesh:ListVirtualGateways",
        "appmesh:ListVirtualNodes",
        "appmesh:ListVirtualRouters",
        "appmesh:ListVirtualServices",
        "apprunner:DescribeService",
        "apprunner:DescribeVpcConnector",
```

```
        "apprunner:ListServices",
        "apprunner:ListTagsForResource",
        "apprunner:ListVpcConnectors",
        "appstream:DescribeAppBlockBuilders",
        "appstream:DescribeApplications",
        "appstream:DescribeDirectoryConfigs",
        "appstream:DescribeFleets",
        "appstream:DescribeStacks",
        "appstream:ListTagsForResource",
        "appsync:GetApiCache",
        "appsync:GetGraphqlApi",
        "appsync:ListGraphqlApis",
        "aps:DescribeAlertManagerDefinition",
        "aps:DescribeLoggingConfiguration",
        "APS:DescribeRuleGroupsNamespace",
        "APS:DescribeWorkspace",
        "aps:ListRuleGroupsNamespaces",
        "aps:ListTagsForResource",
        "APS:ListWorkspaces",
        "athena:GetDataCatalog",
        "athena:GetPreparedStatement",
        "athena:GetWorkGroup",
        "athena:ListDataCatalogs",
        "athena:ListPreparedStatements",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups",
        "auditmanager:GetAccountStatus",
        "auditmanager:GetAssessment",
        "auditmanager:ListAssessments",
        "autoscaling-plans:DescribeScalingPlanResources",
        "autoscaling-plans:DescribeScalingPlans",
        "autoscaling-plans:GetScalingPlanResourceForecastData",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeLaunchConfigurations",
        "autoscaling:DescribeLifecycleHooks",
        "autoscaling:DescribePolicies",
        "autoscaling:DescribeScheduledActions",
        "autoscaling:DescribeTags",
        "autoscaling:DescribeWarmPool",
        "b2bi:GetPartnership",
        "b2bi:GetProfile",
        "b2bi:ListPartnerships",
        "b2bi:ListProfiles",
        "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:GetAgent",
        "bedrock:GetAgentActionGroup",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:GetDataSource",
        "bedrock:GetFlowAlias",
        "bedrock:GetFlowVersion",
        "bedrock:GetGuardrail",
        "bedrock:GetInferenceProfile",
        "bedrock:GetKnowledgeBase",
        "bedrock:ListAgentActionGroups",
        "bedrock:ListAgentKnowledgeBases",
        "bedrock:ListAgents",
        "bedrock:ListDataSources",
```

```
        "bedrock:ListFlowAliases",
        "bedrock:ListFlowVersions",
        "bedrock:ListGuardrails",
        "bedrock:ListInferenceProfiles",
        "bedrock:ListKnowledgeBases",
        "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:GetAnomalyMonitors",
        "ce:GetAnomalySubscriptions",
        "cleanrooms-ml:GetTrainingDataset",
        "cleanrooms-ml:ListTrainingDatasets",
        "cleanrooms:GetConfiguredTable",
        "cleanrooms:GetConfiguredTableAnalysisRule",
        "cleanrooms:GetMembership",
        "cleanrooms:GetPrivacyBudgetTemplate",
        "cleanrooms:ListConfiguredTables",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListPrivacyBudgetTemplates",
        "cloud9:DescribeEnvironmentMemberships",
        "cloud9:DescribeEnvironments",
        "cloud9:ListEnvironments",
        "cloud9:ListTagsForResource",
        "cloudformation:BatchDescribeTypeConfigurations",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeType",
        "cloudformation:GetResource",
        "cloudformation:ListResources",
        "cloudformation:ListStackInstances",
        "cloudformation:ListStackResources",
        "cloudformation:ListStacks",
        "cloudformation:ListStackSets",
        "cloudformation:ListTypes",
```

```
        "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:GetEventDataStore",
        "cloudtrail:GetEventSelectors",
        "cloudtrail:GetInsightSelectors",
        "cloudtrail:GetTrailStatus",
        "cloudTrail:ListChannels",
        "cloudtrail:ListEventDataStores",
        "cloudtrail:ListTags",
        "cloudtrail:ListTrails",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:DescribeAnomalyDetectors",
        "cloudwatch:GetDashboard",
        "cloudwatch:GetMetricStream",
        "cloudwatch:ListDashboards",
        "cloudwatch:ListMetricStreams",
        "cloudwatch:ListTagsForResource",
        "codeartifact:DescribeRepository",
        "codeartifact:GetRepositoryPermissionsPolicy",
        "codeartifact:ListDomains",
        "codeartifact:ListPackages",
        "codeartifact:ListPackageVersions",
        "codeartifact:ListRepositories",
        "codeartifact:ListTagsForResource",
        "codebuild:BatchGetReportGroups",
        "codebuild:ListReportGroups",
        "codecommit:GetRepository",
        "codecommit:GetRepositoryTriggers",
        "codecommit:ListRepositories",
        "codecommit:ListTagsForResource",
        "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:ListPipelines",
        "cognito-identity:DescribeIdentityPool",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:GetPrincipalTagAttributeMap",
        "cognito-identity:ListIdentityPools",
        "cognito-identity:ListTagsForResource",
        "cognito-idp:DescribeIdentityProvider",
        "cognito-idp:DescribeResourceServer",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:DescribeUserPoolDomain",
        "cognito-idp:GetGroup",
        "cognito-idp:GetUserPoolMfaConfig",
        "cognito-idp:ListGroups",
        "cognito-idp:ListIdentityProviders",
        "cognito-idp:ListResourceServers",
        "cognito-idp:ListTagsForResource",
        "cognito-idp:ListUserPoolClients",
        "cognito-idp:ListUserPools",
        "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:DescribePrompt",
```

```
        "connect:DescribeQueue",
        "connect:DescribeQuickConnect",
        "connect:DescribeRoutingProfile",
        "connect:DescribeRule",
        "connect:DescribeSecurityProfile",
        "connect:DescribeUser",
        "connect:GetTaskTemplate",
        "connect:ListApprovedOrigins",
        "connect:ListEvaluationForms",
        "connect:ListInstanceAttributes",
        "connect:ListInstances",
        "connect:ListInstanceStorageConfigs",
        "connect:ListIntegrationAssociations",
        "connect:ListPhoneNumbers",
        "connect:ListPhoneNumbersV2",
        "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:ListUsers",
        "connect:SearchAvailablePhoneNumbers",
        "databrew:DescribeDataset",
        "databrew:DescribeJob",
        "databrew:DescribeProject",
        "databrew:DescribeRecipe",
        "databrew:DescribeRuleset",
        "databrew:DescribeSchedule",
        "databrew:ListDatasets",
        "databrew:ListJobs",
        "databrew:ListProjects",
        "databrew:ListRecipes",
        "databrew:ListRecipeVersions",
        "databrew:ListRulesets",
        "databrew:ListSchedules",
        "datasync:DescribeAgent",
```

```
        "datasync:DescribeLocationEfs",
        "datasync:DescribeLocationFsxLustre",
        "datasync:DescribeLocationFsxWindows",
        "datasync:DescribeLocationHdfs",
        "datasync:DescribeLocationNfs",
        "datasync:DescribeLocationObjectStorage",
        "datasync:DescribeLocationS3",
        "datasync:DescribeLocationSmb",
        "datasync:DescribeTask",
        "datasync:ListAgents",
        "datasync:ListLocations",
        "datasync:ListTagsForResource",
        "datasync:ListTasks",
        "datazone:GetDomain",
        "datazone:ListDomains",
        "dax:DescribeClusters",
        "dax:DescribeParameterGroups",
        "dax:DescribeParameters",
        "dax:DescribeSubnetGroups",
        "dax:ListTags",
        "detective:ListGraphs",
        "detective:ListTagsForResource",
        "devicefarm:GetInstanceProfile",
        "devicefarm:GetNetworkProfile",
        "devicefarm:GetProject",
        "devicefarm:GetTestGridProject",
        "devicefarm:ListInstanceProfiles",
        "devicefarm:ListNetworkProfiles",
        "devicefarm:ListProjects",
        "devicefarm:ListTagsForResource",
        "devicefarm:ListTestGridProjects",
        "devops-guru:GetResourceCollection",
        "devops-guru:ListNotificationChannels",
        "directconnect:DescribeConnections",
        "dms:DescribeCertificates",
        "dms:DescribeEndpoints",
        "dms:DescribeEventSubscriptions",
        "dms:DescribeReplicationConfigs",
        "dms:DescribeReplicationInstances",
        "dms:DescribeReplicationSubnetGroups",
        "dms:DescribeReplicationTaskAssessmentRuns",
        "dms:DescribeReplicationTasks",
        "dms:ListTagsForResource",
        "ds:DescribeDirectories",
```

```
        "ds:DescribeDomainControllers",
        "ds:DescribeEventTopics",
        "ds:ListLogSubscriptions",
        "ds:ListTagsForResource",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeGlobalTable",
        "dynamodb:DescribeGlobalTableSettings",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeTableReplicaAutoScaling",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:ListTables",
        "dynamodb:ListTagsOfResource",
        "ec2:Describe*",
        "ec2:DescribeClientVpnAuthorizationRules",
        "ec2:DescribeClientVpnEndpoints",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeFleets",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSpotFleetRequests",
        "ec2:DescribeTags",
        "ec2:DescribeTrafficMirrorFilters",
        "ec2:DescribeTrafficMirrorSessions",
        "ec2:DescribeTrafficMirrorTargets",
        "ec2:DescribeVolumeAttribute",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcEndpoints",
        "ec2:GetAllowedImagesSettings",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetInstanceTypesFromInstanceRequirements",
        "ec2:GetIpamPoolAllocations",
        "ec2:GetIpamPoolCidrs",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetNetworkInsightsAccessScopeAnalysisFindings",
        "ec2:GetNetworkInsightsAccessScopeContent",
        "ec2:GetSnapshotBlockPublicAccessState",
        "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:DescribeAddon",
        "eks:DescribeCluster",
        "eks:DescribeFargateProfile",
        "eks:DescribeIdentityProviderConfig",
        "eks:DescribeNodegroup",
        "eks:ListAddons",
        "eks:ListClusters",
        "eks:ListFargateProfiles",
        "eks:ListIdentityProviderConfigs",
        "eks:ListNodegroups",
        "eks:ListTagsForResource",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeCacheParameterGroups",
        "elasticache:DescribeCacheParameters",
        "elasticache:DescribeCacheSecurityGroups",
        "elasticache:DescribeCacheSubnetGroups",
        "elasticache:DescribeGlobalReplicationGroups",
        "elasticache:DescribeReplicationGroups",
        "elasticache:DescribeSnapshots",
        "elasticache:DescribeUserGroups",
        "elasticache:DescribeUsers",
        "elasticache:ListTagsForResource",
        "elasticbeanstalk:DescribeConfigurationSettings",
        "elasticbeanstalk:DescribeEnvironments",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeBackupPolicy",
        "elasticfilesystem:DescribeFileSystemPolicy",
```

```
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeMountTargetSecurityGroups",
        "elasticfilesystem:DescribeTags",
        "elasticloadbalancing:DescribeListenerCertificates",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancerPolicies",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:DescribeSecurityConfiguration",
        "elasticmapreduce:DescribeStep",
        "elasticmapreduce:DescribeStudio",
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:GetManagedScalingPolicy",
        "elasticmapreduce:GetStudioSessionMapping",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListInstanceFleets",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListSecurityConfigurations",
        "elasticmapreduce:ListSteps",
        "elasticmapreduce:ListStudios",
        "elasticmapreduce:ListStudioSessionMappings",
        "emr-containers: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:GetSchemaMapping",
        "entityresolution:ListIdMappingWorkflows",
        "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:DescribeFleetAttributes",
        "gamelift:DescribeFleetCapacity",
        "gamelift:DescribeFleetLocationAttributes",
        "gamelift:DescribeFleetLocationCapacity",
        "gamelift:DescribeFleetPortSettings",
        "gamelift:DescribeGameServerGroup",
        "gamelift:DescribeGameSessionQueues",
        "gamelift:DescribeMatchmakingConfigurations",
        "gamelift:DescribeMatchmakingRuleSets",
        "gamelift:DescribeRuntimeConfiguration",
        "gamelift:DescribeScript",
        "gamelift:DescribeVpcPeeringAuthorizations",
        "gamelift:DescribeVpcPeeringConnections",
        "gamelift:ListAliases",
        "gamelift:ListBuilds",
        "gamelift:ListFleets",
        "gamelift:ListGameServerGroups",
        "gamelift:ListScripts",
        "gamelift:ListTagsForResource",
        "geo:DescribeGeofenceCollection",
        "geo:DescribeMap",
        "geo:DescribePlaceIndex",
        "geo:DescribeRouteCalculator",
```

```
        "geo:DescribeTracker",
        "geo:ListGeofenceCollections",
        "geo:ListMaps",
        "geo:ListPlaceIndexes",
        "geo:ListRouteCalculators",
        "geo:ListTrackerConsumers",
        "geo:ListTrackers",
        "globalaccelerator:DescribeAccelerator",
        "globalaccelerator:DescribeEndpointGroup",
        "globalaccelerator:DescribeListener",
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListEndpointGroups",
        "globalaccelerator:ListListeners",
        "globalaccelerator:ListTagsForResource",
        "glue:BatchGetDevEndpoints",
        "glue:BatchGetJobs",
        "glue:BatchGetWorkflows",
        "glue:GetClassifier",
        "glue:GetClassifiers",
        "glue:GetCrawler",
        "glue:GetCrawlers",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetDevEndpoint",
        "glue:GetDevEndpoints",
        "glue:GetJob",
        "glue:GetJobs",
        "glue:GetMLTransform",
        "glue:GetMLTransforms",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue: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:GetMasterAccount",
        "guardduty:GetMemberDetectors",
        "guardduty:GetMembers",
        "guardduty:GetThreatIntelSet",
        "guardduty:ListDetectors",
        "guardduty:ListFilters",
        "guardduty:ListFindings",
        "guardduty:ListIPSets",
        "guardduty:ListMembers",
        "guardduty:ListOrganizationAdminAccounts",
        "guardduty:ListPublishingDestinations",
        "guardduty:ListTagsForResource",
        "guardduty:ListThreatIntelSets",
        "healthlake:DescribeFHIRDatastore",
        "healthlake:ListFHIRDatastores",
        "healthlake:ListTagsForResource",
        "iam:GenerateCredentialReport",
        "iam:GetAccountAuthorizationDetails",
        "iam:GetAccountPasswordPolicy",
        "iam:GetAccountSummary",
        "iam:GetCredentialReport",
        "iam:GetGroup",
```

```
        "iam:GetGroupPolicy",
        "iam:GetInstanceProfile",
        "iam:GetOpenIDConnectProvider",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:GetSAMLProvider",
        "iam:GetServerCertificate",
        "iam:GetUser",
        "iam:GetUserPolicy",
        "iam:ListAccessKeys",
        "iam:ListAttachedGroupPolicies",
        "iam:ListAttachedRolePolicies",
        "iam:ListAttachedUserPolicies",
        "iam:ListEntitiesForPolicy",
        "iam:ListGroupPolicies",
        "iam:ListGroups",
        "iam:ListGroupsForUser",
        "iam:ListInstanceProfiles",
        "iam:ListInstanceProfilesForRole",
        "iam:ListInstanceProfileTags",
        "iam:ListMFADevices",
        "iam:ListMFADeviceTags",
        "iam:ListOpenIDConnectProviders",
        "iam:ListPolicyVersions",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListSAMLProviders",
        "iam:ListServerCertificates",
        "iam:ListUserPolicies",
        "iam:ListUsers",
        "iam:ListVirtualMFADevices",
        "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: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",
        "iot:DescribeAccountAuditConfiguration",
        "iot:DescribeAuthorizer",
        "iot:DescribeBillingGroup",
        "iot:DescribeCACertificate",
        "iot:DescribeCertificate",
        "iot:DescribeCustomMetric",
        "iot:DescribeDimension",
        "iot:DescribeDomainConfiguration",
        "iot:DescribeFleetMetric",
        "iot:DescribeJobTemplate",
        "iot:DescribeMitigationAction",
        "iot:DescribeProvisioningTemplate",
        "iot:DescribeRoleAlias",
        "iot:DescribeScheduledAudit",
        "iot:DescribeSecurityProfile",
        "iot:DescribeThingGroup",
        "iot:DescribeThingType",
        "iot:GetPolicy",
        "iot:GetTopicRule",
        "iot:GetTopicRuleDestination",
        "iot:ListAuthorizers",
        "iot:ListBillingGroups",
        "iot:ListCACertificates",
        "iot:ListCertificates",
        "iot:ListCustomMetrics",
        "iot:ListDimensions",
        "iot:ListDomainConfigurations",
        "iot:ListFleetMetrics",
        "iot:ListJobTemplates",
```

```
        "iot:ListMitigationActions",
        "iot:ListPolicies",
        "iot:ListProvisioningTemplates",
        "iot:ListRoleAliases",
        "iot:ListScheduledAudits",
        "iot:ListSecurityProfiles",
        "iot:ListSecurityProfilesForTarget",
        "iot:ListTagsForResource",
        "iot:ListTargetsForSecurityProfile",
        "iot: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:ListAssetModels",
        "iotsitewise:ListAssets",
        "iotsitewise:ListDashboards",
        "iotsitewise:ListGateways",
        "iotsitewise:ListPortals",
        "iotsitewise:ListProjectAssets",
        "iotsitewise:ListProjects",
        "iotsitewise:ListTagsForResource",
        "iottwinmaker:GetComponentType",
        "iottwinmaker:GetEntity",
        "iottwinmaker:GetScene",
        "iottwinmaker:GetSyncJob",
        "iottwinmaker:GetWorkspace",
        "iottwinmaker:ListComponentTypes",
        "iottwinmaker:ListEntities",
        "iottwinmaker:ListScenes",
        "iottwinmaker:ListSyncJobs",
        "iottwinmaker:ListTagsForResource",
        "iottwinmaker:ListWorkspaces",
        "iotwireless:GetDestination",
        "iotwireless:GetDeviceProfile",
        "iotwireless:GetFuotaTask",
        "iotwireless:GetMulticastGroup",
        "iotwireless:GetServiceProfile",
        "iotwireless:GetWirelessDevice",
        "iotwireless:GetWirelessGateway",
        "iotwireless:GetWirelessGatewayTaskDefinition",
        "iotwireless:ListDestinations",
        "iotwireless:ListDeviceProfiles",
        "iotwireless:ListFuotaTasks",
        "iotwireless:ListMulticastGroups",
        "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: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:ListConnectors",
        "kendra:DescribeIndex",
        "kendra:ListIndices",
        "kendra:ListTagsForResource",
        "kinesis:DescribeStreamConsumer",
```

```
        "kinesis:DescribeStreamSummary",
        "kinesis:ListStreamConsumers",
        "kinesis:ListStreams",
        "kinesis:ListTagsForStream",
        "kinesisanalytics:DescribeApplication",
        "kinesisanalytics:ListApplications",
        "kinesisanalytics:ListTagsForResource",
        "kinesisvideo:DescribeSignalingChannel",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:ListSignalingChannels",
        "kinesisvideo:ListStreams",
        "kinesisvideo:ListTagsForResource",
        "kinesisvideo:ListTagsForStream",
        "kms:DescribeKey",
        "kms:GetKeyPolicy",
        "kms:GetKeyRotationStatus",
        "kms:ListAliases",
        "kms:ListKeys",
        "kms:ListResourceTags",
        "lakeformation:DescribeResource",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:ListPermissions",
        "lakeformation:ListResources",
        "lambda:GetAlias",
        "lambda:GetCodeSigningConfig",
        "lambda:GetEventSourceMapping",
        "lambda:GetFunction",
        "lambda:GetFunctionCodeSigningConfig",
        "lambda:GetLayerVersion",
        "lambda:GetPolicy",
        "lambda:ListAliases",
        "lambda:ListCodeSigningConfigs",
        "lambda:ListEventSourceMappings",
        "lambda:ListFunctions",
        "lambda:ListLayers",
        "lambda:ListLayerVersions",
        "lambda:ListTags",
        "lambda:ListVersionsByFunction",
        "lex:DescribeBot",
        "lex:DescribeBotAlias",
        "lex:DescribeBotVersion",
        "lex:DescribeResourcePolicy",
        "lex:ListBotAliases",
        "lex:ListBotLocales",
```

```
        "lex:ListBots",
        "lex:ListBotVersions",
        "lex:ListTagsForResource",
        "license-manager:GetGrant",
        "license-manager:GetLicense",
        "license-manager:ListDistributedGrants",
        "license-manager:ListLicenses",
        "license-manager:ListReceivedGrants",
        "lightsail:GetAlarms",
        "lightsail:GetBuckets",
        "lightsail:GetCertificates",
        "lightsail:GetContainerServices",
        "lightsail:GetDisk",
        "lightsail:GetDisks",
        "lightsail:GetDistributions",
        "lightsail:GetInstance",
        "lightsail:GetInstances",
        "lightsail:GetKeyPair",
        "lightsail:GetLoadBalancer",
        "lightsail:GetLoadBalancers",
        "lightsail:GetLoadBalancerTlsCertificates",
        "lightsail:GetRelationalDatabase",
        "lightsail:GetRelationalDatabaseParameters",
        "lightsail:GetRelationalDatabases",
        "lightsail:GetStaticIp",
        "lightsail:GetStaticIps",
        "logs:DescribeAccountPolicies",
        "logs:DescribeDestinations",
        "logs:DescribeLogGroups",
        "logs:DescribeMetricFilters",
        "logs:DescribeResourcePolicies",
        "logs:GetDataProtectionPolicy",
        "logs:GetLogAnomalyDetector",
        "logs:GetLogDelivery",
        "logs:ListLogAnomalyDetectors",
        "logs:ListLogDeliveries",
        "logs:ListTagsLogGroup",
        "lookoutequipment:DescribeInferenceScheduler",
        "lookoutequipment:ListTagsForResource",
        "lookoutmetrics:DescribeAlert",
        "lookoutmetrics:DescribeAnomalyDetector",
        "lookoutmetrics:ListAlerts",
        "lookoutmetrics:ListAnomalyDetectors",
        "lookoutmetrics:ListMetricSets",
```

```
        "lookoutmetrics:ListTagsForResource",
        "lookoutvision:DescribeProject",
        "lookoutvision:ListProjects",
        "m2:GetEnvironment",
        "m2:ListEnvironments",
        "m2:ListTagsForResource",
        "macie2:DescribeOrganizationConfiguration",
        "macie2:GetAutomatedDiscoveryConfiguration",
        "macie2:GetClassificationExportConfiguration",
        "macie2:GetCustomDataIdentifier",
        "macie2:GetFindingsPublicationConfiguration",
        "macie2:GetMacieSession",
        "macie2: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",
        "mediapackage-vod:DescribePackagingConfiguration",
        "mediapackage-vod:DescribePackagingGroup",
        "mediapackage-vod:ListPackagingConfigurations",
        "mediapackage-vod:ListPackagingGroups",
        "mediapackage-vod:ListTagsForResource",
        "mediapackagev2:GetChannel",
        "mediapackagev2:ListChannels",
        "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",
        "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:GetDirectoryRegistration",
        "pca-connector-ad:ListDirectoryRegistrations",
        "pca-connector-ad:ListTagsForResource",
        "personalize:DescribeDataset",
        "personalize:DescribeDatasetGroup",
        "personalize:DescribeSchema",
        "personalize:DescribeSolution",
        "personalize:ListDatasetGroups",
        "personalize:ListDatasetImportJobs",
        "personalize:ListDatasets",
        "personalize:ListSchemas",
        "personalize:ListSolutions",
        "personalize:ListTagsForResource",
        "profile:GetDomain",
        "profile:GetIntegration",
        "profile:GetProfileObjectType",
        "profile:ListDomains",
        "profile:ListIntegrations",
        "profile:ListProfileObjectTypes",
        "profile:ListTagsForResource",
        "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:DescribeTemplate",
        "quicksight:DescribeTemplatePermissions",
        "quicksight:DescribeTheme",
        "quicksight:DescribeThemePermissions",
```

```
        "quicksight:ListAnalyses",
        "quicksight:ListDashboards",
        "quicksight:ListDataSets",
        "quicksight:ListDataSources",
        "quicksight:ListTagsForResource",
        "quicksight:ListTemplates",
        "quicksight:ListThemes",
        "ram:GetPermission",
        "ram:GetResourceShareAssociations",
        "ram:GetResourceShares",
        "ram:ListPermissionAssociations",
        "ram:ListPermissions",
        "ram:ListPermissionVersions",
        "ram:ListResources",
        "ram:ListResourceSharePermissions",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBProxies",
        "rds:DescribeDBProxyEndpoints",
        "rds:DescribeDBProxyTargetGroups",
        "rds:DescribeDBProxyTargets",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBShardGroups",
        "rds:DescribeDBSnapshotAttributes",
        "rds:DescribeDBSnapshots",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultClusterParameters",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeGlobalClusters",
        "rds:DescribeIntegrations",
        "rds:DescribeOptionGroups",
        "rds:ListTagsForResource",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:ListWorkgroups",
```

```
        "redshift:DescribeClusterParameterGroups",
        "redshift:DescribeClusterParameters",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSecurityGroups",
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeClusterSubnetGroups",
        "redshift:DescribeEndpointAccess",
        "redshift:DescribeEndpointAuthorization",
        "redshift:DescribeEventSubscriptions",
        "redshift:DescribeIntegrations",
        "redshift:DescribeLoggingStatus",
        "redshift:DescribeScheduledActions",
        "redshift:DescribeTags",
        "refactor-spaces:GetEnvironment",
        "refactor-spaces:GetService",
        "refactor-spaces:ListApplications",
        "refactor-spaces:ListEnvironments",
        "refactor-spaces:ListServices",
        "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",
        "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:GetAccessGrantsInstance",
        "s3:GetAccessGrantsLocation",
        "s3:GetAccessPoint",
        "s3:GetAccessPointForObjectLambda",
        "s3:GetAccessPointPolicy",
        "s3:GetAccessPointPolicyForObjectLambda",
        "s3:GetAccessPointPolicyStatus",
        "s3:GetAccessPointPolicyStatusForObjectLambda",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketCORS",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketNotification",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketRequestPayment",
```

```
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "s3:GetBucketWebsite",
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetMultiRegionAccessPoint",
        "s3:GetMultiRegionAccessPointPolicy",
        "s3:GetMultiRegionAccessPointPolicyStatus",
        "s3:GetReplicationConfiguration",
        "s3:GetStorageLensConfiguration",
        "s3:GetStorageLensConfigurationTagging",
        "s3:GetStorageLensGroup",
        "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:ListTableBuckets",
        "sagemaker:DescribeAppImageConfig",
        "sagemaker:DescribeCluster",
        "sagemaker:DescribeCodeRepository",
        "sagemaker:DescribeDataQualityJobDefinition",
        "sagemaker:DescribeDeviceFleet",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeFeatureGroup",
        "sagemaker:DescribeImage",
        "sagemaker:DescribeImageVersion",
        "sagemaker:DescribeInferenceExperiment",
        "sagemaker:DescribeMlflowTrackingServer",
        "sagemaker:DescribeModel",
```

```
        "sagemaker:DescribeModelBiasJobDefinition",
        "sagemaker:DescribeModelExplainabilityJobDefinition",
        "sagemaker:DescribeModelQualityJobDefinition",
        "sagemaker:DescribeMonitoringSchedule",
        "sagemaker:DescribeNotebookInstance",
        "sagemaker:DescribeNotebookInstanceLifecycleConfig",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribeProject",
        "sagemaker:DescribeStudioLifecycleConfig",
        "sagemaker:DescribeWorkteam",
        "sagemaker:ListAppImageConfigs",
        "sagemaker:ListClusters",
        "sagemaker:ListCodeRepositories",
        "sagemaker:ListDataQualityJobDefinitions",
        "sagemaker:ListDeviceFleets",
        "sagemaker:ListDomains",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListEndpoints",
        "sagemaker:ListFeatureGroups",
        "sagemaker:ListImages",
        "sagemaker:ListImageVersions",
        "sagemaker:ListInferenceExperiments",
        "sagemaker:ListMlflowTrackingServers",
        "sagemaker:ListModelBiasJobDefinitions",
        "sagemaker:ListModelExplainabilityJobDefinitions",
        "sagemaker:ListModelQualityJobDefinitions",
        "sagemaker:ListModels",
        "sagemaker:ListMonitoringSchedules",
        "sagemaker:ListNotebookInstanceLifecycleConfigs",
        "sagemaker:ListNotebookInstances",
        "sagemaker:ListPipelines",
        "sagemaker:ListProjects",
        "sagemaker:ListStudioLifecycleConfigs",
        "sagemaker:ListTags",
        "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:ListSecrets",
        "secretsmanager:ListSecretVersionIds",
        "securityhub:DescribeHub",
        "securityhub:DescribeStandardsControls",
        "securityhub:GetEnabledStandards",
        "serviceCatalog:DescribePortfolioShares",
        "servicediscovery:GetInstance",
        "servicediscovery:GetNamespace",
        "servicediscovery:GetService",
        "servicediscovery:ListInstances",
        "servicediscovery:ListNamespaces",
        "servicediscovery:ListServices",
        "servicediscovery:ListTagsForResource",
        "ses:DescribeReceiptRule",
        "ses:DescribeReceiptRuleSet",
        "ses:GetConfigurationSet",
        "ses:GetConfigurationSetEventDestinations",
        "ses:GetContactList",
        "ses:GetDedicatedIpPool",
        "ses:GetDedicatedIps",
        "ses:GetEmailTemplate",
        "ses:GetTemplate",
        "ses:ListConfigurationSets",
        "ses:ListContactLists",
        "ses:ListDedicatedIpPools",
        "ses:ListEmailTemplates",
        "ses:ListReceiptFilters",
        "ses:ListReceiptRuleSets",
        "ses:ListTemplates",
        "shield:DescribeDRTAccess",
        "shield:DescribeProtection",
        "shield:DescribeSubscription",
        "signer:GetSigningProfile",
        "signer:ListProfilePermissions",
        "signer:ListSigningProfiles",
        "sns:GetDataProtectionPolicy",
        "sns:GetSMSSandboxAccountStatus",
        "sns:GetSubscriptionAttributes",
        "sns:GetTopicAttributes",
```

```
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTagsForResource",
        "sns:ListTopics",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues",
        "sqs:ListQueueTags",
        "ssm-contacts:GetContact",
        "ssm-contacts:GetContactChannel",
        "ssm-contacts:ListContactChannels",
        "ssm-contacts:ListContacts",
        "ssm-incidents:GetResponsePlan",
        "ssm-incidents:ListResponsePlans",
        "ssm-incidents:ListTagsForResource",
        "ssm-quicksetup:GetConfigurationManager",
        "ssm-quicksetup:ListConfigurationManagers",
        "ssm-sap:ListTagsForResource",
        "ssm:DescribeAutomationExecutions",
        "ssm:DescribeDocument",
        "ssm:DescribeDocumentPermission",
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeParameters",
        "ssm:GetAutomationExecution",
        "ssm:GetDocument",
        "ssm:GetServiceSetting",
        "ssm:ListDocuments",
        "ssm:ListTagsForResource",
        "sso:DescribeInstanceAccessControlAttributeConfiguration",
        "sso:DescribePermissionSet",
        "sso:GetInlinePolicyForPermissionSet",
        "sso:ListManagedPoliciesInPermissionSet",
        "sso:ListPermissionSets",
        "sso:ListTagsForResource",
        "states:DescribeActivity",
        "states:DescribeStateMachine",
        "states:ListActivities",
        "states:ListStateMachines",
        "states:ListTagsForResource",
        "storagegateway:ListGateways",
        "storagegateway:ListTagsForResource",
        "storagegateway:ListVolumes",
        "sts:GetCallerIdentity",
        "support:DescribeCases",
        "synthetics:DescribeCanaries",
```

```
        "synthetics:DescribeCanariesLastRun",
        "synthetics:DescribeRuntimeVersions",
        "synthetics:GetCanary",
        "synthetics:GetCanaryRuns",
        "synthetics:GetGroup",
        "synthetics:ListAssociatedGroups",
        "synthetics:ListGroupResources",
        "synthetics:ListGroups",
        "synthetics:ListTagsForResource",
        "tag:GetResources",
        "timestream:DescribeDatabase",
        "timestream:DescribeEndpoints",
        "timestream:DescribeTable",
        "timestream:ListDatabases",
        "timestream:ListTables",
        "timestream:ListTagsForResource",
        "transfer:DescribeAgreement",
        "transfer:DescribeCertificate",
        "transfer:DescribeConnector",
        "transfer:DescribeProfile",
        "transfer:DescribeServer",
        "transfer:DescribeUser",
        "transfer:DescribeWorkflow",
        "transfer:ListAgreements",
        "transfer:ListCertificates",
        "transfer:ListConnectors",
        "transfer:ListProfiles",
        "transfer:ListServers",
        "transfer:ListTagsForResource",
        "transfer:ListUsers",
        "transfer:ListWorkflows",
        "voiceid:DescribeDomain",
        "voiceid:ListTagsForResource",
        "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:ListRuleGroups",
        "wafv2:ListTagsForResource",
        "workspaces:DescribeConnectionAliases",
        "workspaces:DescribeTags",
        "workspaces:DescribeWorkspaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConfigLogStreamStatementID",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/config/*"
    },
    {
      "Sid" : "ConfigLogEventsStatementID",
      "Effect" : "Allow",
      "Action" : "logs:PutLogEvents",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/config/*:log-stream:config-rule-
evaluation/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSAccountActivityAccess

Deskripsi: Memungkinkan pengguna mengakses halaman Aktivitas Akun.

`AWSAccountActivityAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSAccountActivityAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu telah diedit: 07 Maret 2023, 17:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountActivityAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
        "account:GetAlternateContact",
        "account:GetChallengeQuestions",
        "account:GetContactInformation",
        "account:GetRegionOptStatus",
        "account:ListRegions",
        "billing:GetIAMAccessPreference",
```

```
        "billing:GetSellerOfRecord",
        "payments:ListPaymentPreferences"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-portal:ViewBilling"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSAccountManagementFullAccess

Deskripsi: Menyediakan akses penuh ke Manajemen AWS Akun.

`AWSAccountManagementFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSAccountManagementFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 September 2021 23:20 UTC
- Waktu yang telah diedit: 30 September 2021, 23:20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountManagementFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSAccountManagementReadOnlyAccess

Deskripsi: Menyediakan akses hanya-baca ke Manajemen Akun AWS

`AWSAccountManagementReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSAccountManagementReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 September 2021 23:29 UTC
- Waktu yang telah diedit: 30 September 2021, 23:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountManagementReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSAccountUsageReportAccess

Deskripsi: Memungkinkan pengguna mengakses halaman Laporan Penggunaan Akun.

`AWSAccountUsageReportAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSAccountUsageReportAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu telah diedit: 06 Februari 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountUsageReportAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSAgentlessDiscoveryService

Deskripsi: Menyediakan akses untuk Discovery Agentless Connector untuk mendaftar dengan AWS Application Discovery Service.

`AWSAgentlessDiscoveryService`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSAgentlessDiscoveryService` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 02 Agustus 2016, 01:35 UTC
- Waktu yang telah diedit: 24 Februari 2020, 23:08 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAgentlessDiscoveryService`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "awsconnector:RegisterConnector",
        "awsconnector:GetConnectorHealth"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:GetUser",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::connector-platform-upgrade-info/*",
        "arn:aws:s3:::connector-platform-upgrade-info",
        "arn:aws:s3:::connector-platform-upgrade-bundles/*",
        "arn:aws:s3:::connector-platform-upgrade-bundles",
        "arn:aws:s3:::connector-platform-release-notes/*",
        "arn:aws:s3:::connector-platform-release-notes",
        "arn:aws:s3:::prod.agentless.discovery.connector.upgrade/*",
        "arn:aws:s3:::prod.agentless.discovery.connector.upgrade"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource" : [
        "arn:aws:s3:::import-to-ec2-connector-debug-logs/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "SNS:Publish"
      ],
      "Resource" : "arn:aws:sns:*:*:metrics-sns-topic-for-*"
    },
    {
      "Sid" : "Discovery",
      "Effect" : "Allow",
      "Action" : [
        "Discovery:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "arsenal",
      "Effect" : "Allow",
      "Action" : [
        "arsenal:RegisterOnPremisesAgent"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:GetHomeRegion"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSAppFabricFullAccess

Deskripsi: Menyediakan akses penuh ke AWS AppFabric layanan dan hanya membaca akses ke layanan dependen seperti S3, Kinesis, KMS.

`AWSAppFabricFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSAppFabricFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Juni 2023, 19:51 UTC
- Waktu yang telah diedit: 27 Juni 2023, 19:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppFabricFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3ReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "FirehoseReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowUseOfServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "appfabric.amazonaws.com"
        }
      },
      "Resource" : "arn:aws:iam::*:role/aws-service-role/appfabric.amazonaws.com/
AWSServiceRoleForAppFabric"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSAppFabricReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke AWS AppFabric

`AWSAppFabricReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSAppFabricReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Juni 2023, 19:52 UTC
- Waktu yang telah diedit: 27 Juni 2023, 19:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppFabricReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
    {
      "Effect" : "Allow",
      "Action" : [
        "appfabric:GetAppAuthorization",
        "appfabric:GetAppBundle",
        "appfabric:GetIngestion",
        "appfabric:GetIngestionDestination",
        "appfabric:ListAppAuthorizations",
        "appfabric:ListAppBundles",
        "appfabric:ListIngestionDestinations",
        "appfabric:ListIngestions",
        "appfabric:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSAppFabricServiceRolePolicy

Deskripsi: Menyediakan AppFabric akses ke AWS sumber daya atas nama Anda

`AWSAppFabricServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan

- Waktu pembuatan: 26 Juni 2023, 21:07 UTC
- Waktu yang telah diedit: 26 Juni 2023, 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAppFabricServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchEmitMetric",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/AppFabric"
        }
      }
    },
    {
      "Sid" : "S3PutObject",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::*/AWSAppFabric/*",
      "Condition" : {
        "StringEquals" : {
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Sid" : "FirehosePutRecord",
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecordBatch"
      ],
      "Resource" : "arn:aws:firehose:*:*:deliverystream/*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "aws:ResourceTag/AWSAppFabricManaged" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSApplicationAutoscalingAppStreamFleetPolicy

Deskripsi: Kebijakan yang memberikan izin untuk Application Auto Scaling untuk mengakses dan. AppStream CloudWatch

`AWSApplicationAutoscalingAppStreamFleetPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan

- Waktu pembuatan: 20 Oktober 2017, 19:04 UTC
- Waktu telah diedit: 20 Oktober 2017, 19:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingAppStreamFleetPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appstream:UpdateFleet",
        "appstream:DescribeFleets",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSApplicationAutoscalingCassandraTablePolicy

Deskripsi: Kebijakan yang memberikan izin untuk Application Auto Scaling untuk mengakses Cassandra dan. CloudWatch

`AWSApplicationAutoscalingCassandraTablePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 18 Maret 2020, 22:49 UTC
- Waktu diedit: 18 Maret 2020, 22:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingCassandraTablePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
        "arn:*:cassandra:*:*:/keyspace/system/table/*",
        "arn:*:cassandra:*:*:/keyspace/system_schema/table/*",
        "arn:*:cassandra:*:*:/keyspace/system_schema_mcs/table/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cassandra:Alter",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSApplicationAutoscalingComprehendEndpointPolicy

Deskripsi: Kebijakan yang memberikan izin untuk Application Auto Scaling untuk mengakses Comprehend dan. CloudWatch

`AWSApplicationAutoscalingComprehendEndpointPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan

- Waktu pembuatan: 14 November 2019, 18:39 UTC
- Waktu yang telah diedit: 14 November 2019, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingComprehendEndpointPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "comprehend:UpdateEndpoint",
        "comprehend:DescribeEndpoint",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSApplicationAutoScalingCustomResourcePolicy

Deskripsi: Kebijakan yang memberikan izin untuk Application Auto Scaling untuk APIGateway mengakses CloudWatch dan untuk penskalaan sumber daya kustom

`AWSApplicationAutoScalingCustomResourcePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 04 Juni 2018, 23:22 UTC
- Waktu yang telah diedit: 04 Juni 2018, 23:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoScalingCustomResourcePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
        "execute-api:Invoke",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSApplicationAutoscalingDynamoDBTablePolicy

Deskripsi: Kebijakan yang memberikan izin untuk Application Auto Scaling untuk mengakses DynamoDB dan. CloudWatch

`AWSApplicationAutoscalingDynamoDBTablePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 20 Oktober 2017, 21:34 UTC
- Waktu telah diedit: 20 Oktober 2017, 21:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingDynamoDBTablePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeTable",
        "dynamodb:UpdateTable",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSApplicationAutoscalingEC2SpotFleetRequestPolicy

Deskripsi: Kebijakan yang memberikan izin untuk Application Auto Scaling untuk EC2 mengakses Armada Spot dan. CloudWatch

`AWSApplicationAutoscalingEC2SpotFleetRequestPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 25 Oktober 2017, 18:23 UTC
- Waktu yang telah diedit: 25 Oktober 2017, 18:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingEC2SpotFleetRequestPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSpotFleetRequests",
        "ec2:ModifySpotFleetRequest",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSApplicationAutoscalingECSServicePolicy

Deskripsi: Kebijakan yang memberikan izin untuk Application Auto Scaling untuk EC2 mengakses Layanan Kontainer dan. CloudWatch

`AWSApplicationAutoscalingECSServicePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 25 Oktober 2017, 23:53 UTC
- Waktu yang telah diedit: 24 Oktober 2024, 20:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingECSServicePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeServices",
        "ecs:UpdateService",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSApplicationAutoscalingElastiCacheRGPolicy

Deskripsi: Kebijakan yang memberikan izin untuk Application Auto Scaling untuk mengakses Amazon dan Amazon ElastiCache . CloudWatch

`AWSApplicationAutoscalingElastiCacheRGPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 17 Agustus 2021 23:41 UTC
- Waktu telah diedit: 26 Maret 2025, 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingElastiCacheRGPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSApplicationAutoscalingEMRInstanceGroupPolicy

Deskripsi: Kebijakan yang memberikan izin untuk Application Auto Scaling untuk mengakses Elastic Map Reduce dan. CloudWatch

`AWSApplicationAutoscalingEMRInstanceGroupPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 26 Oktober 2017, 00:57 UTC
- Waktu yang telah diedit: 26 Oktober 2017, 00:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingEMRInstanceGroupPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ModifyInstanceGroups",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSApplicationAutoscalingKafkaClusterPolicy

Deskripsi: Kebijakan yang memberikan izin untuk Application Auto Scaling untuk mengakses Managed Streaming for Apache Kafka dan. CloudWatch

`AWSApplicationAutoscalingKafkaClusterPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 24 Agustus 2020, 18:36 UTC
- Waktu yang telah diedit: 24 Agustus 2020, 18:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingKafkaClusterPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
        "kafka:UpdateBrokerStorage",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSApplicationAutoscalingLambdaConcurrencyPolicy

Deskripsi: Kebijakan yang memberikan izin untuk Application Auto Scaling untuk mengakses Lambda dan. CloudWatch

`AWSApplicationAutoscalingLambdaConcurrencyPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 21 Oktober 2019, 20:04 UTC
- Waktu yang telah diedit: 21 Oktober 2019, 20:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingLambdaConcurrencyPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:PutProvisionedConcurrencyConfig",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:DeleteProvisionedConcurrencyConfig",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSApplicationAutoscalingNeptuneClusterPolicy

Deskripsi: Kebijakan yang memberikan izin untuk Application Auto Scaling untuk mengakses Amazon Neptunus dan Amazon. CloudWatch

`AWSApplicationAutoscalingNeptuneClusterPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 02 September 2021 21:14 UTC
- Waktu yang telah diedit: 02 September 2021 21:14 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingNeptuneClusterPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "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*"
```

```
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSApplicationAutoscalingRDSClusterPolicy

Deskripsi: Kebijakan yang memberikan izin untuk Application Auto Scaling untuk mengakses RDS dan. CloudWatch

`AWSApplicationAutoscalingRDSClusterPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 17 Oktober 2017, 17:46 UTC
- Waktu telah diedit: 07 Agustus 2018, 19:14 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingRDSClusterPolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSApplicationAutoscalingSageMakerEndpointPolicy

Deskripsi: Kebijakan yang memberikan izin untuk Application Auto Scaling untuk mengakses dan. SageMaker CloudWatch

`AWSApplicationAutoscalingSageMakerEndpointPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 06 Februari 2018, 19:58 UTC
- Waktu telah diedit: 13 November 2023, 18:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingSageMakerEndpointPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeInferenceComponent",
        "sagemaker:UpdateEndpointWeightsAndCapacities",
        "sagemaker:UpdateInferenceComponentRuntimeConfig",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SageMakerCloudWatchUpdate",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:TargetTracking*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSApplicationAutoscalingWorkSpacesPoolPolicy

Deskripsi: Kebijakan yang memberikan izin untuk Application Auto Scaling untuk mengakses Amazon dan Amazon WorkSpaces . CloudWatch

`AWSApplicationAutoscalingWorkSpacesPoolPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 17 Juni 2024, 18:39 UTC
- Waktu yang telah diedit: 17 Juni 2024, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingWorkSpacesPoolPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSApplicationDiscoveryAgentAccess

Deskripsi: Menyediakan akses bagi Discovery Agent untuk mendaftar dengan AWS Application Discovery Service.

`AWSApplicationDiscoveryAgentAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSApplicationDiscoveryAgentAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 11 Mei 2016, 21:38 UTC
- Waktu yang telah diedit: 24 Februari 2020, 22:26 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationDiscoveryAgentAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:GetHomeRegion"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSApplicationDiscoveryAgentlessCollectorAccess

Deskripsi: Memungkinkan Application Discovery Service Agentless Collectors untuk memperbarui, mendaftar, dan berkomunikasi secara otomatis dengan Application Discovery Service

`AWSApplicationDiscoveryAgentlessCollectorAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSApplicationDiscoveryAgentlessCollectorAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 16 Agustus 2022, 21:00 UTC
- Waktu yang telah diedit: 16 Agustus 2022, 21.00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationDiscoveryAgentlessCollectorAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "arsenal:RegisterOnPremisesAgent"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr-public:DescribeImages"
      ],
      "Resource" : "arn:aws:ecr-
public::446372222237:repository/6e5498e4-8c31-4f57-9991-13b4b992ff7b"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr-public:GetAuthorizationToken"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:GetHomeRegion"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "sts:GetServiceBearerToken"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSApplicationDiscoveryServiceFullAccess

Deskripsi: Menyediakan akses penuh untuk melihat dan menandai Item Konfigurasi yang dikelola oleh AWS Application Discovery Service

`AWSApplicationDiscoveryServiceFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSApplicationDiscoveryServiceFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 11 Mei 2016, 21:30 UTC
- Waktu yang telah diedit: 19 Juni 2019, 21:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationDiscoveryServiceFullAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mgh:*",
        "discovery:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "iam:GetRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
continuousexport.discovery.amazonaws.com/
AWSServiceRoleForApplicationDiscoveryServiceContinuousExport*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "continuousexport.discovery.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
```

```
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
continuousexport.discovery.amazonaws.com/
AWSServiceRoleForApplicationDiscoveryServiceContinuousExport*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "migrationhub.amazonaws.com",
            "dmsintegration.migrationhub.amazonaws.com",
            "smsintegration.migrationhub.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSApplicationMigrationAgentInstallationPolicy

Deskripsi: Kebijakan ini memungkinkan penginstalan Agen AWS Replikasi, yang digunakan dengan AWS Application Migration Service (MGN) untuk memigrasikan server eksternal. AWS Lampirkan kebijakan ini ke pengguna IAM atau peran yang kredensialnya Anda berikan saat menginstal Agen Replikasi. AWS

`AWSApplicationMigrationAgentInstallationPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSApplicationMigrationAgentInstallationPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 19 Juni 2022, 07:51 UTC
- Waktu yang telah diedit: 20 September 2022, 11.21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationAgentInstallationPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:GetAgentInstallationAssetsForMgn",
        "mgn:SendClientMetricsForMgn",
        "mgn:SendClientLogsForMgn",
        "mgn:RegisterAgentForMgn",
        "mgn:VerifyClientRoleForMgn"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "mgn:IssueClientCertificateForMgn"
      ],
      "Resource" : "arn:aws:mgn:*:*:source-server/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "mgn:TagResource",
      "Resource" : "arn:aws:mgn:*:*:source-server/*",
      "Condition" : {
        "StringEquals" : {
          "mgn:CreateAction" : "RegisterAgentForMgn"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSApplicationMigrationAgentPolicy

Deskripsi: Kebijakan ini memungkinkan penginstalan dan penggunaan Agen AWS Replikasi, yang digunakan dengan AWS Application Migration Service (MGN) untuk memigrasikan server eksternal ke. AWS Lampirkan kebijakan ini ke pengguna IAM atau peran yang kredensialnya Anda berikan saat menginstal Agen Replikasi. AWS

`AWSApplicationMigrationAgentPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSApplicationMigrationAgentPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 07 April 2021, 07:00 UTC
- Waktu yang telah diedit: 20 September 2022, 11.13 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationAgentPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:SendAgentMetricsForMgn",
        "mgn:SendAgentLogsForMgn",
        "mgn:SendClientMetricsForMgn",
        "mgn:SendClientLogsForMgn"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:RegisterAgentForMgn",
        "mgn:UpdateAgentSourcePropertiesForMgn",
        "mgn:UpdateAgentReplicationInfoForMgn",
        "mgn:UpdateAgentConversionInfoForMgn",
        "mgn:GetAgentInstallationAssetsForMgn",
        "mgn:GetAgentCommandForMgn",
        "mgn:GetAgentConfirmedResumeInfoForMgn",
```

```
        "mgn:GetAgentRuntimeConfigurationForMgn",
        "mgn:UpdateAgentBacklogForMgn",
        "mgn:GetAgentReplicationInfoForMgn"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "mgn:TagResource",
      "Resource" : "arn:aws:mgn:*:*:source-server/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSApplicationMigrationAgentPolicy_v2

Deskripsi: Kebijakan ini memungkinkan penggunaan Agen AWS Replikasi, yang digunakan dengan AWS Application Migration Service (MGN) untuk memigrasikan server eksternal ke. AWS Kami tidak menyarankan Anda melampirkan kebijakan ini ke pengguna atau peran IAM Anda.

`AWSApplicationMigrationAgentPolicy_v2`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSApplicationMigrationAgentPolicy_v2` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 06 Juni 2022, 14:14 UTC

- Waktu yang telah diedit: 06 Juni 2022, 14.14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationAgentPolicy_v2`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:SendAgentMetricsForMgn",
        "mgn:SendAgentLogsForMgn",
        "mgn:UpdateAgentSourcePropertiesForMgn",
        "mgn:UpdateAgentReplicationInfoForMgn",
        "mgn:UpdateAgentConversionInfoForMgn",
        "mgn:GetAgentCommandForMgn",
        "mgn:GetAgentConfirmedResumeInfoForMgn",
        "mgn:GetAgentRuntimeConfigurationForMgn",
        "mgn:UpdateAgentBacklogForMgn",
        "mgn:GetAgentReplicationInfoForMgn",
        "mgn:IssueClientCertificateForMgn"
      ],
      "Resource" : "arn:aws:mgn:*:*:source-server/${aws:SourceIdentity}"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSApplicationMigrationConversionServerPolicy

Deskripsi: Kebijakan ini memungkinkan Server Konversi Layanan Migrasi Aplikasi (MGN), yang merupakan EC2 instance yang diluncurkan oleh Layanan Migrasi Aplikasi, untuk berkomunikasi dengan layanan MGN. Peran IAM dengan kebijakan ini dilampirkan (sebagai Profil EC2 Instance) oleh MGN ke Server Konversi MGN, yang secara otomatis diluncurkan dan dihentikan oleh MGN, bila diperlukan. Kami tidak menyarankan Anda melampirkan kebijakan ini ke pengguna atau peran IAM Anda. Server Konversi MGN digunakan oleh Layanan Migrasi Aplikasi saat pengguna memilih untuk meluncurkan instance Test atau Cutover menggunakan konsol MGN, CLI, atau API.

`AWSApplicationMigrationConversionServerPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSApplicationMigrationConversionServerPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 07 April 2021, 06:48 UTC
- Waktu yang telah diedit: 07 April 2021, 06:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationConversionServerPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:SendClientMetricsForMgn",
        "mgn:SendClientLogsForMgn",
        "mgn:GetChannelCommandsForMgn",
        "mgn:SendChannelCommandResultForMgn"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSApplicationMigrationEC2Access

Deskripsi: Kebijakan ini menyediakan EC2 operasi Amazon yang diperlukan untuk menggunakan Application Migration Service (MGN) untuk meluncurkan server yang dimigrasi sebagai EC2 instance. Lampirkan kebijakan ini ke pengguna atau peran IAM Anda.

`AWSApplicationMigrationEC2Access`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSApplicationMigrationEC2Access` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 07 April 2021, 07:05 UTC
- Waktu yang telah diedit: 11 Februari 2025, 13:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationEC2Access`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AWSApplicationMigrationConversionServerRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
```

```
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSnapshots",
        "ec2:DescribeImages",
        "ec2:DescribeVolumes"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
```

```
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteLaunchTemplate"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:GetConsoleOutput",
        "ec2:GetConsoleScreenshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
```

```
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateSecurityGroup",
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "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"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSApplicationMigrationFullAccess

Deskripsi: Kebijakan ini memberikan izin kepada semua publik Layanan APIs Migrasi AWS Aplikasi (MGN), serta izin untuk membaca informasi kunci KMS. Lampirkan kebijakan ini ke pengguna atau peran IAM Anda.

`AWSApplicationMigrationFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSApplicationMigrationFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 07 April 2021, 06:56 UTC
- Waktu yang telah diedit: 02 Juli 2025, 15:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationFullAccess`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSApplicationMigrationMGHAccess

Deskripsi: Kebijakan ini memungkinkan Layanan Migrasi AWS Aplikasi (MGN) untuk mengirim meta-data tentang kemajuan server yang dimigrasi menggunakan MGN ke Migration AWS Hub (MGH). MGN secara otomatis membuat peran IAM dengan kebijakan ini terlampir, dan mengambil peran ini. Kami tidak menyarankan Anda melampirkan kebijakan ini ke pengguna atau peran IAM Anda.

`AWSApplicationMigrationMGHAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSApplicationMigrationMGHAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 07 April 2021, 07:10 UTC
- Waktu telah diedit: 07 April 2021, 07:10 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationMGHAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:AssociateCreatedArtifact",
        "mgh:CreateProgressUpdateStream",
        "mgh:DisassociateCreatedArtifact",
        "mgh:GetHomeRegion",
        "mgh:ImportMigrationTask",
        "mgh:NotifyMigrationTaskState",
        "mgh:PutResourceAttributes"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSApplicationMigrationReadOnlyAccess

Deskripsi: Kebijakan ini memberikan izin kepada semua publik hanya-baca Layanan APIs Migrasi Aplikasi (MGN), serta beberapa AWS layanan hanya-baca APIs lainnya yang diperlukan untuk menggunakan konsol MGN hanya-baca sepenuhnya. Lampirkan kebijakan ini ke pengguna atau peran IAM Anda.

`AWSApplicationMigrationReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSApplicationMigrationReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 07 April 2021, 07:15 UTC
- Waktu telah diedit: 20 Maret 2023, 08:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:DescribeJobLogItems",
        "mgn:DescribeJobs",
        "mgn:DescribeSourceServers",
        "mgn:DescribeReplicationConfigurationTemplates",
        "mgn:GetLaunchConfiguration",
        "mgn:DescribeVcenterClients",
        "mgn:GetReplicationConfiguration",
        "mgn:DescribeLaunchConfigurationTemplates",
        "mgn:ListSourceServerActions",
        "mgn:ListTemplateActions",
        "mgn:ListApplications",
        "mgn:ListWaves",
        "mgn:ListExports",
        "mgn:ListImports",
        "mgn:ListImportErrors",
        "mgn:ListExportErrors"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSApplicationMigrationReplicationServerPolicy

Deskripsi: Kebijakan ini memungkinkan Server Replikasi Layanan Migrasi Aplikasi (MGN), yang merupakan EC2 instance yang diluncurkan oleh Layanan Migrasi Aplikasi - untuk berkomunikasi dengan layanan MGN, dan untuk membuat snapshot EBS di aplikasi Anda. Akun AWS Peran IAM dengan kebijakan ini dilampirkan (sebagai Profil EC2 Instance) oleh Layanan Migrasi Aplikasi ke Server Replikasi MGN yang secara otomatis diluncurkan dan dihentikan oleh MGN, sesuai kebutuhan. Server Replikasi MGN digunakan untuk memfasilitasi replikasi data dari server eksternal Anda ke AWS, sebagai bagian dari proses migrasi yang dikelola menggunakan MGN. Kami tidak menyarankan Anda melampirkan kebijakan ini ke pengguna atau peran IAM Anda.

`AWSApplicationMigrationReplicationServerPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSApplicationMigrationReplicationServerPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 07 April 2021, 07:21 UTC
- Waktu yang telah diedit: 07 April 2021, 07:21 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationReplicationServerPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:SendClientMetricsForMgn",
        "mgn:SendClientLogsForMgn",
        "mgn:GetChannelCommandsForMgn",
        "mgn:SendChannelCommandResultForMgn",
        "mgn:GetAgentSnapshotCreditsForMgn",
        "mgn:DescribeReplicationServerAssociationsForMgn",
        "mgn:DescribeSnapshotRequestsForMgn",
        "mgn:BatchDeleteSnapshotRequestForMgn",
        "mgn:NotifyAgentAuthenticationForMgn",
        "mgn:BatchCreateVolumeSnapshotGroupForMgn",
        "mgn:UpdateAgentReplicationProcessStateForMgn",
        "mgn:NotifyAgentReplicationProgressForMgn",
        "mgn:NotifyAgentConnectedForMgn",
        "mgn:NotifyAgentDisconnectedForMgn"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateSnapshot"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSApplicationMigrationServiceEc2InstancePolicy

Deskripsi: Kebijakan ini memungkinkan penginstalan dan penggunaan Agen AWS Replikasi, yang digunakan oleh AWS Application Migration Service (AWS MGN) untuk memigrasikan server sumber yang berjalan di EC2 (Lintas wilayah atau lintas AZ). Peran IAM dengan kebijakan ini harus dilampirkan (sebagai Profil EC2 Instance) ke EC2 Instans.

`AWSApplicationMigrationServiceEc2InstancePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSApplicationMigrationServiceEc2InstancePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 22 Agustus 2023, 13:19 UTC
- Waktu telah diedit: 03 Januari 2024, 14:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationServiceEc2InstancePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      "Effect" : "Allow",
      "Action" : [
        "mgn:SendClientLogsForMgn",
        "mgn:RegisterAgentForMgn",
        "mgn:GetAgentInstallationAssetsForMgn"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MgnAgentReplication",
      "Effect" : "Allow",
      "Action" : [
        "mgn:SendAgentMetricsForMgn",
        "mgn:SendAgentLogsForMgn",
        "mgn:UpdateAgentSourcePropertiesForMgn",
        "mgn:UpdateAgentReplicationInfoForMgn",
        "mgn:UpdateAgentConversionInfoForMgn",
        "mgn:GetAgentCommandForMgn",
        "mgn:GetAgentConfirmedResumeInfoForMgn",
        "mgn:GetAgentRuntimeConfigurationForMgn",
        "mgn:UpdateAgentBacklogForMgn",
        "mgn:GetAgentReplicationInfoForMgn"
      ],
      "Resource" : "arn:aws:mgn:*:*:source-server/*"
    },
    {
      "Sid" : "MgnSourceServerTagResource",
      "Effect" : "Allow",
      "Action" : "mgn:TagResource",
      "Resource" : "arn:aws:mgn:*:*:source-server/*",
      "Condition" : {
        "StringEquals" : {
          "mgn:CreateAction" : "RegisterAgentForMgn"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSApplicationMigrationServiceRolePolicy

Deskripsi: Memungkinkan Layanan Migrasi AWS aplikasi untuk membuat dan mengelola AWS sumber daya atas nama Anda.

`AWSApplicationMigrationServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 07 April 2021, 06:43 UTC
- Waktu telah diedit: 16 Maret 2025, 10:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationMigrationServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      "Effect" : "Allow",
      "Action" : "mgn:ListTagsForResource",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "kms:ListRetirableGrants",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:AssociateCreatedArtifact",
        "mgh:CreateProgressUpdateStream",
        "mgh:DisassociateCreatedArtifact",
        "mgh:GetHomeRegion",
        "mgh:ImportMigrationTask",
        "mgh:NotifyMigrationTaskState",
        "mgh:PutResourceAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstanceAttribute",
        "ec2: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"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSApplicationMigrationSSMAccess

Deskripsi: Kebijakan ini menyediakan akses ke operasi SSM Amazon yang diperlukan untuk menggunakan Layanan Migrasi Aplikasi (MGN) untuk menjalankan perintah pasca migrasi kustom dokumen SSM. Lampirkan kebijakan ini ke pengguna atau peran IAM Anda.

`AWSApplicationMigrationSSMAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSApplicationMigrationSSMAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 November 2022, 09:29 UTC
- Waktu yang telah diedit: 02 Juli 2025, 18:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationSSMAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetCommandInvocation",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:DescribeDocument",
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/*",
        "arn:aws:ssm:*:*:automation-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/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSApplicationMigrationVCenterClientPolicy

Deskripsi: Kebijakan ini memungkinkan penginstalan dan penggunaan AWS VCenter Klien, yang digunakan dengan Layanan Migrasi AWS Aplikasi (MGN) untuk memigrasikan server eksternal. AWS Lampirkan kebijakan ini ke pengguna atau peran IAM Anda yang kredensialnya Anda berikan saat menginstal Klien. AWS VCenter

`AWSApplicationMigrationVCenterClientPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSApplicationMigrationVCenterClientPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 08 November 2021 12:53 UTC
- Waktu yang telah diedit: 08 November 2021, 12:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationVCenterClientPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:CreateVcenterClientForMgn",
        "mgn:DescribeVcenterClients"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:GetVcenterClientCommandsForMgn",
        "mgn:SendVcenterClientCommandResultForMgn",
        "mgn:SendVcenterClientLogsForMgn",
        "mgn:SendVcenterClientMetricsForMgn",
        "mgn:DeleteVcenterClient",
        "mgn:TagResource",
        "mgn:NotifyVcenterClientStartedForMgn"
      ],
      "Resource" : "arn:aws:mgn:*:*:vcenter-client/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSAppMeshEnvoyAccess

Deskripsi: Kebijakan App Mesh Envoy untuk mengakses konfigurasi Virtual Node.

`AWSAppMeshEnvoyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSAppMeshEnvoyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 Juli 2019, 21:29 UTC
- Waktu diedit: 03 Juli 2019, 21:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppMeshEnvoyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSAppMeshFullAccess

Deskripsi: Menyediakan akses penuh ke AWS App Mesh APIs dan Konsol Manajemen.

`AWSAppMeshFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSAppMeshFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 16 April 2019, 17:50 UTC
- Waktu yang telah diedit: 07 Januari 2021, 19:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppMeshFullAccess`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/appmesh.amazonaws.com/
AWSServiceRoleForAppMesh",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : [
            "appmesh.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStack*",
        "cloudformation:UpdateStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/AWSAppMesh-GettingStarted-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:ListCertificates",
        "acm:DescribeCertificate",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:ListCertificateAuthorities"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:ListNamespaces",
        "servicediscovery:ListServices",
        "servicediscovery:ListInstances"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSAppMeshPreviewEnvoyAccess

Deskripsi: Kebijakan Utusan Pratinjau App Mesh untuk mengakses konfigurasi Node Virtual.

`AWSAppMeshPreviewEnvoyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSAppMeshPreviewEnvoyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 05 Agustus 2019, 23:32 UTC
- Waktu telah diedit: 05 Agustus 2019, 23:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppMeshPreviewEnvoyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appmesh-preview:StreamAggregatedResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSAppMeshPreviewServiceRolePolicy

Deskripsi: Mengaktifkan akses ke Layanan AWS dan Sumber Daya yang digunakan atau dikelola oleh AWS App Mesh

`AWSAppMeshPreviewServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 19 Juni 2019, 19:07 UTC
- Waktu yang telah diedit: Agustus 21, 2019, 21:06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAppMeshPreviewServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudMapServiceDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DiscoverInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ACMCertificateVerification",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSAppMeshReadOnly

Deskripsi: Menyediakan akses hanya-baca ke AWS App Mesh APIs dan Konsol Manajemen.

`AWSAppMeshReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSAppMeshReadOnly` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 16 April 2019, 17:51 UTC
- Waktu yang telah diedit: 07 Januari 2021, 19:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppMeshReadOnly`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      "Resource" : "arn:aws:cloudformation:*:*:stack/AWSAppMesh-GettingStarted-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:ListCertificates",
        "acm:DescribeCertificate",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:ListCertificateAuthorities"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:ListNamespaces",
        "servicediscovery:ListServices",
        "servicediscovery:ListInstances"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSAppMeshServiceRolePolicy

Deskripsi: Memungkinkan akses ke Layanan AWS dan Sumber Daya yang digunakan atau dikelola oleh AWS AppMesh

`AWSAppMeshServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 03 Juni 2019, 18:30 UTC
- Waktu yang telah diedit: 10 Oktober 2023, 16:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAppMeshServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudMapServiceDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DiscoverInstances",
        "servicediscovery:DiscoverInstancesRevision"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ACMCertificateVerification",
      "Effect" : "Allow",
      "Action" : [
```

```
        "acm:DescribeCertificate"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSAppRunnerFullAccess

Deskripsi: Memberikan izin untuk semua tindakan Pelari Aplikasi.

`AWSAppRunnerFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSAppRunnerFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 11 Januari 2022, 04:02 UTC
- Waktu yang telah diedit: 11 Januari 2022, 04:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppRunnerFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/apprunner.amazonaws.com/
AWSServiceRoleForAppRunner",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "apprunner.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "apprunner.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AppRunnerAdminAccess",
      "Effect" : "Allow",
      "Action" : "apprunner:*",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSAppRunnerReadOnlyAccess

Deskripsi: Memberikan izin untuk membuat daftar dan melihat detail tentang sumber daya Pelari Aplikasi.

`AWSAppRunnerReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSAppRunnerReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 24 Februari 2022, 21:24 UTC
- Waktu yang telah diedit: 24 Februari 2022, 21.24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppRunnerReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSAppRunnerServicePolicyForECRAccess

Deskripsi: Kebijakan layanan AWS App Runner yang memberikan izin baca ke sumber daya Amazon ECR di akun pelanggan. Gunakan dalam peran yang diteruskan ke App Runner saat membuat atau memperbarui layanan App Runner.

`AWSAppRunnerServicePolicyForECRAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSAppRunnerServicePolicyForECRAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 14 Mei 2021 19:17 UTC
- Waktu yang telah diedit: 14 Mei 2021 19.17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSAppRunnerServicePolicyForECRAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "ecr:DescribeImages",
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSAppSyncAdministrator

Deskripsi: Menyediakan akses administratif ke AppSync layanan, meskipun tidak cukup untuk mengakses melalui konsol.

`AWSAppSyncAdministrator`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSAppSyncAdministrator` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 20 Maret 2018, 21:20 UTC
- Waktu yang telah diedit: 04 November 2019, 19:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppSyncAdministrator`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appsync:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "appsync.amazonaws.com"
          ]
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "appsync.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/appsync.amazonaws.com/
AWSServiceRoleForAppSync*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSAppSyncInvokeFullAccess

Deskripsi: Menyediakan akses pemanggilan penuh ke AppSync layanan - baik melalui konsol maupun secara mandiri

`AWSAppSyncInvokeFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSAppSyncInvokeFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 20 Maret 2018, 21:21 UTC
- Waktu telah diedit: 20 Maret 2018, 21:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppSyncInvokeFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appsync:GraphQL",
        "appsync:GetGraphqlApi",
        "appsync:ListGraphqlApis",
        "appsync:ListApiKeys"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSAppSyncPushToCloudWatchLogs

Deskripsi: Memungkinkan AppSync untuk mendorong log ke CloudWatch akun pengguna.

`AWSAppSyncPushToCloudWatchLogs`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSAppSyncPushToCloudWatchLogs` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 09 April 2018, 19:38 UTC
- Waktu yang telah diedit: 09 April 2018, 19:38 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSAppSyncPushToCloudWatchLogs`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
```

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSAppSyncSchemaAuthor

Deskripsi: Menyediakan akses untuk membuat, memperbarui, dan menanyakan skema.

`AWSAppSyncSchemaAuthor`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSAppSyncSchemaAuthor` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 20 Maret 2018, 21:21 UTC
- Waktu telah diedit: 01 Februari 2023, 18:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppSyncSchemaAuthor`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appsync:GraphQL",
        "appsync:CreateResolver",
        "appsync:CreateType",
        "appsync:DeleteResolver",
        "appsync:DeleteType",
        "appsync:GetResolver",
        "appsync:GetType",
        "appsync:GetDataSource",
        "appsync:GetSchemaCreationStatus",
        "appsync:GetIntrospectionSchema",
        "appsync:GetGraphqlApi",
        "appsync:ListTypes",
        "appsync:ListApiKeys",
        "appsync:ListResolvers",
        "appsync:ListDataSources",
        "appsync:ListGraphqlApis",
        "appsync:StartSchemaCreation",
        "appsync:UpdateResolver",
        "appsync:UpdateType",
        "appsync:TagResource",
        "appsync:UntagResource",
        "appsync:ListTagsForResource",
        "appsync:CreateFunction",
        "appsync:UpdateFunction",
        "appsync:GetFunction",
        "appsync:DeleteFunction",
        "appsync:ListFunctions",
        "appsync:ListResolversByFunction",
        "appsync:EvaluateMappingTemplate",
        "appsync:EvaluateCode"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSAppSyncServiceRolePolicy

Deskripsi: Memungkinkan akses ke AWS layanan dan sumber daya yang digunakan atau dikelola oleh AppSync

`AWSAppSyncServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 21 Januari 2020, 19:56 UTC
- Waktu yang telah diedit: 21 Januari 2020, 19:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAppSyncServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingTargets",
        "xray:GetSamplingRules",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSArtifactAccountSync

Deskripsi: Memungkinkan akses hanya-baca AWS Artifact ke operasi di Organizations. AWS

`AWSArtifactAccountSync`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSArtifactAccountSync` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 10 April 2018, 23:04 UTC

- Waktu yang telah diedit: 10 April 2018, 23:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSArtifactAccountSync`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSArtifactAgreementsFullAccess

Deskripsi: Kebijakan ini memberikan izin penuh untuk membuat daftar, mengunduh, menerima, dan mengakhiri perjanjian AWS Artifak. Ini juga mencakup izin untuk membuat daftar dan mengaktifkan

akses AWS layanan di layanan Organisasi, serta menjelaskan detail organisasi. Selain itu, kebijakan menyediakan kemampuan untuk memeriksa apakah peran terkait layanan yang diperlukan ada dan membuatnya jika tidak

`AWSArtifactAgreementsFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSArtifactAgreementsFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 22 November 2024, 19:36 UTC
- Waktu telah diedit: 22 November 2024, 19:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSArtifactAgreementsFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "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:EnableAWSServiceAccess",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSArtifactAgreementsReadOnlyAccess

Keterangan: Kebijakan ini memberikan akses hanya-baca untuk membuat daftar perjanjian layanan AWS Artifact dan mengunduh perjanjian yang diterima.. Ini juga mencakup izin untuk membuat daftar serta menjelaskan detail organisasi. Selain itu, kebijakan menyediakan kemampuan untuk memeriksa apakah peran terkait layanan yang diperlukan ada.

`AWSArtifactAgreementsReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSArtifactAgreementsReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 22 November 2024, 19:36 UTC
- Waktu telah diedit: 22 November 2024, 19:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSArtifactAgreementsReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSArtifactReportsReadOnlyAccess

Deskripsi: Menyediakan akses hanya-baca ke laporan layanan AWS Artifact.

`AWSArtifactReportsReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSArtifactReportsReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 02 Januari 2024, 22:42 UTC
- Waktu telah diedit: 24 Maret 2025, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSArtifactReportsReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ArtifactReportActions",
      "Effect" : "Allow",
      "Action" : [
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSArtifactServiceRolePolicy

Deskripsi: Memungkinkan AWS Artifact untuk mengumpulkan informasi tentang organisasi melalui layanan Organizations AWS .

`AWSArtifactServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 21 Agustus 2023, 20:27 UTC
- Waktu telah diedit: Agustus 21, 2023, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSArtifactServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSAuditManagerAdministratorAccess

Deskripsi: Menyediakan akses administratif untuk mengaktifkan atau menonaktifkan AWS Audit Manager, memperbarui pengaturan, dan mengelola penilaian, kontrol, dan kerangka kerja

`AWSAuditManagerAdministratorAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSAuditManagerAdministratorAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 11 Desember 2020, 20:02 UTC
- Waktu yang telah diedit: 15 Mei 2024, 23:46 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAuditManagerAdministratorAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
  "Statement" : [
    {
      "Sid" : "AuditManagerAccess",
      "Effect" : "Allow",
      "Action" : [
        "auditmanager:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccountsForParent",
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:ListParents",
        "organizations:ListChildren"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowOnlyAuditManagerIntegration",
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator",
        "organizations:EnableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "organizations:ServicePrincipal" : [
            "auditmanager.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "IAMAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "iam:GetUser",
        "iam:ListUsers",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMAccessCreateSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/auditmanager.amazonaws.com/
AWSServiceRoleForAuditManager*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "auditmanager.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMAccessManageSLR",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:UpdateRoleDescription",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/auditmanager.amazonaws.com/
AWSServiceRoleForAuditManager*"
    },
    {
      "Sid" : "S3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KmsAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListKeys",
        "kms:ListAliases"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KmsCreateGrantAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : "auditmanager.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SNSAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateEventsAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:detail-type" : "Security Hub Findings - Imported"
        },
        "ForAllValues:StringEquals" : {
          "events:source" : [
            "aws.securityhub"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "EventsAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:EnableRule",
        "events:DisableRule",
        "events:ListTargetsByRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver"
    },
    {
      "Sid" : "TagAccess",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ControlCatalogAccess",
      "Effect" : "Allow",
      "Action" : [
        "controlcatalog:ListCommonControls",
        "controlcatalog:ListDomains",
        "controlcatalog:ListObjectives"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSAuditManagerServiceRolePolicy

Deskripsi: Mengaktifkan akses ke Layanan AWS dan Sumber Daya yang digunakan atau dikelola oleh AWS Audit Manager

`AWSAuditManagerServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 08 Desember 2020, 15:12 UTC
- Waktu telah diedit: 24 September 2024, 23:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAuditManagerServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v10 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSAutoScalingPlansEC2AutoScalingPolicy

Deskripsi: Kebijakan yang memberikan izin kepada Auto AWS Scaling untuk memperkirakan kapasitas secara berkala dan menghasilkan tindakan penskalaan terjadwal untuk grup Auto Scaling dalam rencana penskalaan

`AWSAutoScalingPlansEC2AutoScalingPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 23 Agustus 2018, 22:46 UTC
- Waktu telah diedit: 23 Agustus 2018, 22:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAutoScalingPlansEC2AutoScalingPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeScheduledActions",
        "autoscaling:BatchPutScheduledUpdateGroupAction",
        "autoscaling:BatchDeleteScheduledAction"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSBackupAuditAccess

Deskripsi: Kebijakan ini memberikan izin bagi pengguna untuk membuat kontrol dan kerangka kerja yang menentukan harapan mereka terhadap sumber daya dan aktivitas AWS Cadangan, serta untuk mengaudit sumber daya dan aktivitas AWS Cadangan terhadap kontrol dan kerangka kerja yang ditentukan. Kebijakan ini memberikan izin ke AWS Config dan layanan serupa untuk menjelaskan ekspektasi pengguna dalam melakukan audit. Kebijakan ini juga memberikan izin untuk menyampaikan laporan audit ke S3 dan layanan serupa, dan memungkinkan pengguna untuk menemukan dan membuka laporan audit mereka.

`AWSBackupAuditAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSBackupAuditAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 24 Agustus 2021 01:02 UTC
- Waktu yang telah diedit: 10 April 2023, 21:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupAuditAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
        "backup:CreateFramework",
        "backup:UpdateFramework",
        "backup:ListFrameworks",
        "backup:DescribeFramework",
        "backup:DeleteFramework",
        "backup:ListBackupPlans",
        "backup:ListBackupVaults",
        "backup:CreateReportPlan",
        "backup:UpdateReportPlan",
        "backup:ListReportPlans",
        "backup:DescribeReportPlan",
        "backup:DeleteReportPlan",
        "backup:StartReportJob",
        "backup:ListReportJobs",
        "backup:DescribeReportJob"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:DescribeComplianceByConfigRule"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:GetComplianceDetailsByConfigRule"
      ],
      "Resource" : "arn:aws:config:*:*:config-rule/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation"
      ],
      "Resource" : "arn:aws:s3:::*"
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSBackupDataTransferAccess

Deskripsi: Kebijakan ini memungkinkan agen AWS Backint untuk menyelesaikan transfer data cadangan dengan pesawat AWS Backup Storage. Lampirkan kebijakan ini ke peran yang diasumsikan oleh EC2 Instans yang menjalankan SAP HANA dengan agen Backint.

`AWSBackupDataTransferAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSBackupDataTransferAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 10 November 2022, 22:48 UTC
- Waktu telah diedit: 10 November 2022, 22.48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupDataTransferAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "backup-storage:StartObject",
        "backup-storage:PutChunk",
        "backup-storage:GetChunk",
        "backup-storage:ListChunks",
        "backup-storage:ListObjects",
        "backup-storage:GetObjectMetadata",
        "backup-storage:NotifyObjectComplete"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSBackupFullAccess

Deskripsi: Kebijakan ini ditujukan untuk administrator cadangan, memberikan akses penuh ke operasi AWS Backup, termasuk membuat atau mengedit rencana cadangan, menetapkan AWS sumber daya ke rencana cadangan, menghapus cadangan, dan memulihkan cadangan.

`AWSBackupFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSBackupFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 November 2019, 22:21 UTC
- Waktu yang telah diedit: 22 Mei 2025, 00:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupFullAccess`

Versi kebijakan

Versi kebijakan: v20 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AwsBackupAllAccessPermissions",
      "Effect" : "Allow",
      "Action" : "backup:*",
      "Resource" : "*"
    },
    {
      "Sid" : "AwsBackupStorageAllAccessPermissions",
      "Effect" : "Allow",
      "Action" : "backup-storage:*",
      "Resource" : "*"
    },
    {
      "Sid" : "RdsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBSnapshots",
        "rds:ListTagsForResource",
        "rds:DescribeDBInstances",
        "rds:describeDBEngineVersions",
```

```
        "rds:describeOptionGroups",
        "rds:describeOrderableDBInstanceOptions",
        "rds:describeDBSubnetGroups",
        "rds:describeDBClusterSnapshots",
        "rds:describeDBClusters",
        "rds:describeDBParameterGroups",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBInstanceAutomatedBackups",
        "rds:DescribeDBClusterAutomatedBackups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RdsDeletePermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:DeleteDBSnapshot",
        "rds:DeleteDBClusterSnapshot"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DynamoDbPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListBackups",
        "dynamodb:ListTables"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DynamoDbDeleteBackupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DeleteBackup"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "EfsFileSystemPermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeFilesystems"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*"
    },
    {
      "Sid" : "Ec2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes",
        "ec2:describeAvailabilityZones",
        "ec2:DescribeVpcs",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeImages",
        "ec2:DescribeSubnets",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeAddresses"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Ec2DeletePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot",
        "ec2:DeregisterImage"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ResourceGroupTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetTagKeys",
        "tag:GetTagValues",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "StorageGatewayVolumePermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:DescribeCachediSCSIVolumes",
        "storagegateway:DescribeStorediSCSIVolumes"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*/volume/*"
    },
    {
      "Sid" : "StorageGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:ListGateways"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:*"
    },
    {
      "Sid" : "StorageGatewayGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:DescribeGatewayInformation",
        "storagegateway: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" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync

Deskripsi: Memberikan AWS BackupGateway izin untuk menyinkronkan metadata Mesin Virtual atas nama Anda

`AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 15 Desember 2022, 19:43 UTC
- Waktu telah diedit: 15 Desember 2022 19.43 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ListVmTags",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:ListTagsForResource"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:vm/*"
    },
    {
      "Sid" : "VMTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:TagResource",
```

```
        "backup-gateway:UntagResource"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:vm/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSBackupOperatorAccess

Deskripsi: Kebijakan ini memberi pengguna izin untuk menetapkan AWS sumber daya ke paket cadangan, membuat cadangan sesuai permintaan, dan memulihkan cadangan. Kebijakan ini tidak mengizinkan pengguna untuk membuat atau mengedit rencana cadangan atau menghapus cadangan terjadwal setelah dibuat.

`AWSBackupOperatorAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSBackupOperatorAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 November 2019, 22:23 UTC
- Waktu yang telah diedit: 22 Mei 2025, 00:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupOperatorAccess`

Versi kebijakan

Versi kebijakan: v18 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSBackupOrganizationAdminAccess

Deskripsi: Kebijakan ini ditujukan untuk administrator cadangan yang menggunakan manajemen pencadangan lintas akun untuk mengelola pencadangan organisasi.

`AWSBackupOrganizationAdminAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSBackupOrganizationAdminAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 24 Juni 2020, 16:23 UTC
- Waktu yang telah diedit: 18 November 2022, 18.26 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupOrganizationAdminAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DisableAWSServiceAccess",
        "organizations:EnableAWSServiceAccess",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "backup.amazonaws.com"
          ]
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource" : "arn:aws:organizations::*:account/*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:AttachPolicy",
        "organizations:ListPoliciesForTarget",
        "organizations:ListTargetsForPolicy",
        "organizations:DetachPolicy",
        "organizations:DisablePolicyType",
        "organizations:DescribePolicy",
        "organizations:DescribeEffectivePolicy",
        "organizations:ListPolicies",
        "organizations:EnablePolicyType",
        "organizations:CreatePolicy",
        "organizations:UpdatePolicy",
        "organizations:DeletePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "organizations:PolicyType" : [
            "BACKUP_POLICY"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "organizations:ListRoots",
        "organizations:ListParents",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListAccountsForParent",
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListChildren",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganizationalUnit"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSBackupRestoreAccessForSAPHANA

Deskripsi: Menyediakan izin AWS Backup untuk memulihkan cadangan SAP HANA di Amazon EC2

`AWSBackupRestoreAccessForSAPHANA`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSBackupRestoreAccessForSAPHANA` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 10 November 2022, 22:43 UTC
- Waktu telah diedit: 10 November 2022, 22.43 UTC

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

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "backup:Get*",
        "backup:List*",
        "backup:Describe*",
        "backup:StartBackupJob",
        "backup:StartRestoreJob"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:GetOperation",
        "ssm-sap:ListDatabases"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:BackupDatabase",
        "ssm-sap:RestoreDatabase",
        "ssm-sap:UpdateHanaBackupSettings",
        "ssm-sap:GetDatabase",
        "ssm-sap:ListTagsForResource"
```

```
      ],
      "Resource" : "arn:aws:ssm-sap:*:*:*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSBackupSearchOperatorAccess

Deskripsi: Peran operator pencarian memiliki akses untuk membuat indeks cadangan, membuat pencarian metadata cadangan yang telah diindeks. Kebijakan ini berisi izin yang diperlukan untuk fungsi operator pencarian ini.

`AWSBackupSearchOperatorAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSBackupSearchOperatorAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Februari 2025, 21:52 UTC
- Waktu telah diedit: 25 Maret 2025, 19:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupSearchOperatorAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSBackupServiceLinkedRolePolicyForBackup

Deskripsi: Menyediakan izin AWS Backup untuk membuat backup atas nama Anda di seluruh layanan AWS

`AWSBackupServiceLinkedRolePolicyForBackup`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 02 Juni 2020, 23:08 UTC
- Waktu yang telah diedit: 22 Mei 2025, 00:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBackupServiceLinkedRolePolicyForBackup`

Versi kebijakan

Versi kebijakan: v19 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EFSResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:Backup",
        "elasticfilesystem:DescribeTags"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/aws:elasticfilesystem:default-backup" : "enabled"
```

```
        }
      }
    },
    {
      "Sid" : "DescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources",
        "elasticfilesystem:DescribeFileSystems",
        "dynamodb:ListTables",
        "storagegateway:ListVolumes",
        "ec2:DescribeVolumes",
        "ec2:DescribeInstances",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "fsx:DescribeFileSystems",
        "fsx:DescribeVolumes",
        "s3:ListAllMyBuckets",
        "s3:GetBucketTagging"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SnapshotCopyTagPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CopySnapshot"
        }
      }
    },
    {
      "Sid" : "EC2CreateBackupTagPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*::snapshot/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
```

```
            "AWSBackupManagedResource"
          ]
        }
      }
    },
    {
      "Sid" : "EC2CreateTagsPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*::snapshot/*"
      ],
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSBackupManagedResource" : "false"
        }
      }
    },
    {
      "Sid" : "EC2RDSDescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSnapshots",
        "ec2:DescribeSnapshotTierStatus",
        "ec2:DescribeImages",
        "rds:DescribeDBSnapshots",
        "rds:DescribeDBClusterSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EBSCopyPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:CopySnapshot",
      "Resource" : "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Sid" : "EC2CopyPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:CopyImage",
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "EC2ModifyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeregisterImage",
        "ec2:DeleteSnapshot",
        "ec2:ModifySnapshotTier"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSBackupManagedResource" : "false"
        }
      }
    },
    {
      "Sid" : "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" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM

- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSBackupServiceLinkedRolePolicyForBackupTest

Deskripsi: Menyediakan izin AWS Backup untuk membuat backup atas nama Anda di seluruh layanan AWS

`AWSBackupServiceLinkedRolePolicyForBackupTest`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 12 Mei 2020, 17:37 UTC
- Waktu yang telah diedit: 12 Mei 2020, 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBackupServiceLinkedRolePolicyForBackupTest`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSBackupServiceRolePolicyForBackup

Deskripsi: Menyediakan izin AWS Backup untuk membuat backup atas nama Anda di seluruh layanan AWS

`AWSBackupServiceRolePolicyForBackup`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSBackupServiceRolePolicyForBackup` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan

- Waktu pembuatan: 10 Januari 2019, 21:01 UTC
- Waktu yang telah diedit: 22 Mei 2025, 00:37 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBackupServiceRolePolicyForBackup`

Versi kebijakan

Versi kebijakan: v22 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DynamoDBPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeTable",
        "dynamodb:CreateBackup"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*"
    },
    {
      "Sid" : "DynamoDBBackupResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeBackup",
        "dynamodb:DeleteBackup"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*/backup/*"
    },
    {
      "Sid" : "DynamoDBBackupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:AddTagsToResource",
```

```
        "rds:ListTagsForResource",
        "rds:DescribeDBSnapshots",
        "rds:CreateDBSnapshot",
        "rds:CopyDBSnapshot",
        "rds:DescribeDBInstances",
        "rds:CreateDBClusterSnapshot",
        "rds:DescribeDBClusters",
        "rds:DescribeDBClusterSnapshots",
        "rds:CopyDBClusterSnapshot",
        "rds:DescribeDBClusterAutomatedBackups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "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" : [
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "Sid" : "KMSDynamoDBPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "dynamodb.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "KMSPermissions",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "*"
    },
    {
      "Sid" : "KMSCreateGrantPermissions",
      "Effect" : "Allow",
```

```
      "Action" : "kms:CreateGrant",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        }
      }
    },
    {
      "Sid" : "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"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSBackupServiceRolePolicyForIndexing

Deskripsi: Kebijakan yang berisi izin yang diperlukan untuk AWS Backup untuk mengindeks titik pemulihan.

`AWSBackupServiceRolePolicyForIndexing`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSBackupServiceRolePolicyForIndexing` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 17 Desember 2024, 18:37 UTC
- Waktu telah diedit: 17 Desember 2024, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForIndexing`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSBackupServiceRolePolicyForItemRestores

Deskripsi: Kebijakan yang berisi izin yang diperlukan untuk AWS Backup untuk memulihkan item individual di titik pemulihan

`AWSBackupServiceRolePolicyForItemRestores`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSBackupServiceRolePolicyForItemRestores` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 17 Desember 2024, 18:37 UTC
- Waktu yang telah diedit: 17 Desember 2024, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForItemRestores`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSBackupServiceRolePolicyForRestores

Deskripsi: Memberikan izin AWS Backup untuk melakukan pemulihan atas nama Anda di seluruh AWS layanan. Kebijakan ini mencakup izin untuk membuat dan menghapus AWS sumber daya, seperti volume EBS, instans RDS, dan sistem file EFS, yang merupakan bagian dari proses pemulihan.

`AWSBackupServiceRolePolicyForRestores`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSBackupServiceRolePolicyForRestores` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 12 Januari 2019 00:23 UTC
- Waktu yang telah diedit: 22 Mei 2025, 00:37 UTC

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

Versi kebijakan

Versi kebijakan: v23 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DynamoDBPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:Scan",
        "dynamodb:Query",
        "dynamodb:UpdateItem",
        "dynamodb:PutItem",
        "dynamodb:GetItem",
        "dynamodb:DeleteItem",
        "dynamodb:BatchWriteItem",
        "dynamodb:DescribeTable"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*"
    },
    {
      "Sid" : "DynamoDBBackupResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:RestoreTableFromBackup"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*/backup/*"
    },
    {
      "Sid" : "EBSPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateVolume",
        "ec2:DeleteVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "Sid" : "EC2DescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSnapshotTierStatus",
        "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"
      ],
      "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" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSBackupServiceRolePolicyForS3Backup

Deskripsi: Kebijakan yang berisi izin yang diperlukan untuk AWS Backup untuk mencadangkan data di bucket S3 apa pun. Ini termasuk akses baca ke semua objek S3 dan akses dekripsi apa pun untuk semua kunci KMS.

`AWSBackupServiceRolePolicyForS3Backup`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSBackupServiceRolePolicyForS3Backup` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 Februari 2022, 17:40 UTC
- Waktu yang telah diedit: 17 Mei 2024, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForS3Backup`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSBackupServiceRolePolicyForS3Restore

Deskripsi: Kebijakan yang berisi izin yang diperlukan untuk AWS Backup untuk memulihkan cadangan S3 ke bucket. Ini termasuk izin baca/tulis ke semua bucket S3, dan izin untuk dan untuk GenerateDataKey semua kunci KMS. DescribeKey

`AWSBackupServiceRolePolicyForS3Restore`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSBackupServiceRolePolicyForS3Restore` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 Februari 2022, 17:39 UTC
- Waktu telah diedit: 07 Februari 2023, 00:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForS3Restore`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:ListBucketVersions",
        "s3:ListBucket",
        "s3:GetBucketVersioning",
```

```
        "s3:GetBucketLocation",
        "s3:PutBucketVersioning",
        "s3:PutBucketOwnershipControls",
        "s3:GetBucketOwnershipControls"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:DeleteObject",
        "s3:PutObjectVersionAcl",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectTagging",
        "s3:PutObjectTagging",
        "s3:GetObjectAcl",
        "s3:PutObjectAcl",
        "s3:ListMultipartUploadParts",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        }
      }
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSBatchFullAccess

Deskripsi: Menyediakan akses penuh untuk sumber daya AWS Batch.

`AWSBatchFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSBatchFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Desember 2016, 19:35 UTC
- Waktu yang telah diedit: 24 Oktober 2022, 16.09 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBatchFullAccess`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "batch:*",
        "cloudwatch:GetMetricStatistics",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeVpcs",
        "ec2:DescribeImages",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeLaunchTemplateVersions",
        "ecs:DescribeClusters",
        "ecs:Describe*",
        "ecs:List*",
        "eks:DescribeCluster",
        "eks:ListClusters",
        "logs:Describe*",
        "logs:Get*",
        "logs:TestMetricFilter",
        "logs:FilterLogEvents",
        "iam:ListInstanceProfiles",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSBatchServiceRole",
        "arn:aws:iam::*:role/service-role/AWSBatchServiceRole",
        "arn:aws:iam::*:role/ecsInstanceRole",
        "arn:aws:iam::*:instance-profile/ecsInstanceRole",
        "arn:aws:iam::*:role/iaws-ec2-spot-fleet-role",
        "arn:aws:iam::*:role/aws-ec2-spot-fleet-role",
        "arn:aws:iam::*:role/AWSBatchJobRole*"
      ]
    },
    {
```

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSBatchServiceEventTargetRole

Deskripsi: Kebijakan untuk mengaktifkan Target CloudWatch Acara untuk AWS Pengajuan Pekerjaan Batch

`AWSBatchServiceEventTargetRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSBatchServiceEventTargetRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 28 Februari 2018, 22:31 UTC
- Waktu telah diedit: 28 Februari 2018, 22:31 UTC

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

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSBatchServiceRole

Deskripsi: Kebijakan untuk peran layanan AWS Batch yang memungkinkan akses ke layanan terkait termasuk EC2, Penskalaan Otomatis, layanan EC2 Kontainer, dan Log Cloudwatch.

`AWSBatchServiceRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSBatchServiceRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 06 Desember 2016, 19:36 UTC
- Waktu telah diedit: 05 Desember 2023, 18:49 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBatchServiceRole`

Versi kebijakan

Versi kebijakan: v13 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSBatchPolicyStatement1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeImages",
        "ec2:DescribeImageAttribute",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSpotFleetInstances",
        "ec2:DescribeSpotFleetRequests",
```

```
        "ec2:DescribeSpotPriceHistory",
        "ec2:DescribeSpotFleetRequestHistory",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:CreateLaunchTemplate",
        "ec2:DeleteLaunchTemplate",
        "ec2:RequestSpotFleet",
        "ec2:CancelSpotFleetRequests",
        "ec2:ModifySpotFleetRequest",
        "ec2:TerminateInstances",
        "ec2:RunInstances",
        "autoscaling:DescribeAccountLimits",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeLaunchConfigurations",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeScalingActivities",
        "autoscaling:CreateLaunchConfiguration",
        "autoscaling:CreateAutoScalingGroup",
        "autoscaling:UpdateAutoScalingGroup",
        "autoscaling:SetDesiredCapacity",
        "autoscaling:DeleteLaunchConfiguration",
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:CreateOrUpdateTags",
        "autoscaling:SuspendProcesses",
        "autoscaling:PutNotificationConfiguration",
        "autoscaling:TerminateInstanceInAutoScalingGroup",
        "ecs:DescribeClusters",
        "ecs:DescribeContainerInstances",
        "ecs:DescribeTaskDefinition",
        "ecs:DescribeTasks",
        "ecs:ListAccountSettings",
        "ecs:ListClusters",
        "ecs:ListContainerInstances",
        "ecs:ListTaskDefinitionFamilies",
        "ecs:ListTaskDefinitions",
        "ecs:ListTasks",
        "ecs:CreateCluster",
        "ecs:DeleteCluster",
        "ecs:RegisterTaskDefinition",
        "ecs:DeregisterTaskDefinition",
        "ecs:RunTask",
        "ecs:StartTask",
        "ecs:StopTask",
        "ecs:UpdateContainerAgent",
```

```
        "ecs:DeregisterContainerInstance",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogGroups",
        "iam:GetInstanceProfile",
        "iam:GetRole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSBatchPolicyStatement2",
      "Effect" : "Allow",
      "Action" : "ecs:TagResource",
      "Resource" : [
        "arn:aws:ecs:*:*:task/*_Batch_*"
      ]
    },
    {
      "Sid" : "AWSBatchPolicyStatement3",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn",
            "ecs-tasks.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AWSBatchPolicyStatement4",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "spot.amazonaws.com",
```

```
            "spotfleet.amazonaws.com",
            "autoscaling.amazonaws.com",
            "ecs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AWSBatchPolicyStatement5",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "RunInstances"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSBCMDataExportsServiceRolePolicy

Deskripsi: Peran terkait layanan untuk menyediakan Billing and Cost Management Data Exports akses AWS ke data layanan untuk mengekspor data ke lokasi target, seperti Amazon S3, atas nama pelanggan.

`AWSBCMDataExportsServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 10 Juni 2024, 17:40 UTC
- Waktu yang telah diedit: 10 Juni 2024, 17:40 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBCMDataExportsServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CostOptimizationRecommendationAccess",
      "Effect" : "Allow",
      "Action" : [
        "cost-optimization-hub:ListEnrollmentStatuses",
        "cost-optimization-hub:ListRecommendations"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSBillingConductorFullAccess

Deskripsi: Gunakan kebijakan AWSBilling ConductorFullAccess terkelola untuk mengizinkan akses lengkap ke konsol AWS Billing Conductor (ABC) dan APIs. Kebijakan ini memungkinkan pengguna untuk membuat daftar, membuat, dan menghapus sumber daya ABC.

`AWSBillingConductorFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSBillingConductorFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 13 April 2022, 18:02 UTC
- Waktu yang telah diedit: 13 April 2022, 18.02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBillingConductorFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
    {
      "Effect" : "Allow",
      "Action" : [
        "billingconductor:*",
        "organizations:ListAccounts",
        "pricing:DescribeServices"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSBillingConductorReadOnlyAccess

Deskripsi: Gunakan kebijakan AWSBilling ConductorReadOnlyAccess terkelola untuk mengizinkan akses hanya baca ke konsol AWS Billing Conductor (ABC) dan APIs. Kebijakan ini memberikan izin untuk melihat dan mencantumkan semua sumber daya ABC. Itu tidak termasuk kemampuan untuk membuat atau menghapus sumber daya.

`AWSBillingConductorReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSBillingConductorReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 13 April 2022, 18:02 UTC
- Waktu yang telah diedit: 13 April 2022, 18.02 UTC

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

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "billingconductor:List*",
        "organizations:ListAccounts",
        "pricing:DescribeServices"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSBillingReadOnlyAccess

Deskripsi: Memungkinkan pengguna untuk melihat tagihan di Konsol Penagihan.

`AWSBillingReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSBillingReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Agustus 2020, 20:08 UTC
- Waktu yang telah diedit: 12 Maret 2025, 18:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBillingReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v10 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
        "aws-portal:ViewBilling",
        "billing:GetBillingData",
        "billing:GetBillingDetails",
        "billing:GetBillingNotifications",
        "billing:GetBillingPreferences",
        "billing:GetCredits",
        "billing:GetContractInformation",
        "billing:GetIAMAccessPreference",
        "billing:GetSellerOfRecord",
        "billing:ListBillingViews",
        "budgets:ViewBudget",
```

```
        "budgets:DescribeBudgetActionsForBudget",
        "budgets:DescribeBudgetAction",
        "budgets:DescribeBudgetActionsForAccount",
        "budgets:DescribeBudgetActionHistories",
        "ce:DescribeCostCategoryDefinition",
        "ce:GetCostAndUsage",
        "ce:ListCostCategoryDefinitions",
        "ce:ListTagsForResource",
        "ce:ListCostAllocationTags",
        "ce:ListCostAllocationTagBackfillHistory",
        "ce:GetTags",
        "ce:GetDimensionValues",
        "consolidatedbilling:ListLinkedAccounts",
        "consolidatedbilling:GetAccountBillingRole",
        "cur:GetClassicReport",
        "cur:GetClassicReportPreferences",
        "cur:GetUsageReport",
        "cur:DescribeReportDefinitions",
        "freetier:GetFreeTierAlertPreference",
        "freetier:GetFreeTierUsage",
        "invoicing:BatchGetInvoiceProfile",
        "invoicing:GetInvoiceEmailDeliveryPreferences",
        "invoicing:GetInvoicePDF",
        "invoicing:GetInvoiceUnit",
        "invoicing:ListInvoiceSummaries",
        "invoicing:ListInvoiceUnits",
        "invoicing:ListTagsForResource",
        "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" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM

Deskripsi: Kebijakan ini memberikan izin untuk mengontrol AWS sumber daya. Misalnya, untuk memulai dan menghentikan EC2 atau instance RDS dengan menjalankan skrip AWS Systems Manager (SSM).

`AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 25 Mei 2022, 19:03 UTC
- Waktu yang telah diedit: 25 Mei 2022, 19.03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceStatus",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "rds:DescribeDBInstances",
        "rds:StartDBInstance",
        "rds:StopDBInstance"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-definition/AWS-StartEC2Instance:*",
        "arn:aws:ssm:*:*:automation-definition/AWS-StopEC2Instance:*",
        "arn:aws:ssm:*:*:automation-definition/AWS-StartRdsInstance:*",
        "arn:aws:ssm:*:*:automation-definition/AWS-StopRdsInstance:*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSBudgetsActionsWithAWSResourceControlAccess

Deskripsi: Menyediakan akses penuh ke Tindakan AWS Anggaran termasuk menggunakan Tindakan Anggaran untuk mengontrol status sumber daya yang sedang berjalan melalui AWS AWS Management Console

`AWSBudgetsActionsWithAWSResourceControlAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSBudgetsActionsWithAWSResourceControlAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 15 Oktober 2020, 17:19 UTC

- Waktu yang telah diedit: 15 Oktober 2020, 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBudgetsActionsWithAWSResourceControlAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "budgets:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-portal:ViewBilling"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "budgets.amazonaws.com"
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-portal:ModifyBilling",
        "ec2:DescribeInstances",
        "iam:ListGroups",
        "iam:ListPolicies",
        "iam:ListRoles",
        "iam:ListUsers",
        "organizations:ListAccounts",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListPolicies",
        "organizations:ListRoots",
        "rds:DescribeDBInstances",
        "sns:ListTopics"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSBudgetsReadOnlyAccess

Deskripsi: Menyediakan akses hanya baca ke Konsol AWS Anggaran melalui. AWS Management Console

`AWSBudgetsReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSBudgetsReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 15 Oktober 2020, 17:18 UTC
- Waktu yang telah diedit: 17 Juni 2024, 17:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBudgetsReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSBudgetsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-portal:ViewBilling",
        "budgets:ViewBudget",
        "budgets:Describe*",
        "budgets:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSBugBustFullAccess

Deskripsi: Kebijakan IAM ini memberi pengguna akses penuh ke konsol AWS BugBust

`AWSBugBustFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSBugBustFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 24 Juni 2021, 07:03 UTC
- Waktu yang telah diedit: 22 Juli 2021, 20:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBugBustFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CodeGuruReviewerPermission",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-reviewer:DescribeCodeReview",
        "codeguru-reviewer:ListRecommendations",
```

```
        "codeguru-reviewer:ListCodeReviews"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeGuruProfilerPermission",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-profiler:ListProfilingGroups",
        "codeguru-profiler:DescribeProfilingGroup"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSBugBustFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "bugbust:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSBugBustSLRCreation",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/bugbust.amazonaws.com/
AWSServiceRoleForBugBust",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "bugbust.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSBugBustPlayerAccess

Deskripsi: Kebijakan IAM ini memberi pengguna akses untuk berpartisipasi dalam acara AWS BugBust

`AWSBugBustPlayerAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSBugBustPlayerAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 24 Juni 2021, 07:15 UTC
- Waktu yang telah diedit: 24 Juni 2021, 07:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBugBustPlayerAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CodeGuruReviewerPermission",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-reviewer:DescribeCodeReview",
        "codeguru-reviewer:ListRecommendations"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "CodeGuruProfilerPermission",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-profiler:DescribeProfilingGroup"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSBugBustPlayerAccess",
      "Effect" : "Allow",
      "Action" : [
        "bugbust:ListBugs",
        "bugbust:ListProfilingGroups",
        "bugbust:JoinEvent",
        "bugbust:GetEvent",
        "bugbust:ListEvents",
        "bugbust:GetJoinEventStatus",
        "bugbust:ListEventScores",
        "bugbust:ListEventParticipants",
        "bugbust:UpdateWorkItem",
        "bugbust:ListPullRequests"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSBugBustServiceRolePolicy

Deskripsi: Memberikan izin AWS BugBust untuk mengakses sumber daya atas nama Anda

`AWSBugBustServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 24 Juni 2021 06:59 UTC
- Waktu telah diedit: 24 Juni 2021 06:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBugBustServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codeguru-reviewer:ListRecommendations",
        "codeguru-reviewer:UntagResource",
        "codeguru-reviewer:DescribeCodeReview"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/bugbust" : "enabled"
```

```
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCertificateManagerFullAccess

Deskripsi: Menyediakan akses penuh ke AWS Certificate Manager (ACM)

`AWSCertificateManagerFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCertificateManagerFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 21 Januari 2016, 17:02 UTC
- Waktu yang telah diedit: 17 Agustus 2020, 22:18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/acm.amazonaws.com/
AWSServiceRoleForCertificateManager*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "acm.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus",
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/acm.amazonaws.com/
AWSServiceRoleForCertificateManager*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCertificateManagerPrivateCAAuditor

Deskripsi: Menyediakan akses auditor ke AWS Certificate Manager Private Certificate Authority

`AWSCertificateManagerPrivateCAAuditor`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCertificateManagerPrivateCAAuditor` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 23 Oktober 2018, 16:51 UTC
- Waktu yang telah diedit: 17 Agustus 2020, 22:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAAuditor`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:CreateCertificateAuthorityAuditReport",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:DescribeCertificateAuthorityAuditReport",
```

```
        "acm-pca:GetCertificateAuthorityCsr",
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:GetPolicy",
        "acm-pca:ListPermissions",
        "acm-pca:ListTags"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:ListCertificateAuthorities"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCertificateManagerPrivateCAFullAccess

Deskripsi: Menyediakan akses penuh ke AWS Certificate Manager Private Certificate Authority

`AWSCertificateManagerPrivateCAFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCertificateManagerPrivateCAFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 23 Oktober 2018, 16:54 UTC
- Waktu telah diedit: 23 Oktober 2018, 16:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCertificateManagerPrivateCAPrivilegedUser

Deskripsi: Menyediakan akses pengguna sertifikat istimewa ke Certificate Manager AWS Private Certificate Authority

`AWSCertificateManagerPrivateCAPrivilegedUser`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCertificateManagerPrivateCAPrivilegedUser` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 20 Juni 2019, 17:43 UTC
- Waktu telah diedit: 22 Januari 2025, 19:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAPrivilegedUser`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCertificateManagerPrivateCAReadOnly

Deskripsi: Menyediakan akses baca saja ke AWS Certificate Manager Private Certificate Authority

`AWSCertificateManagerPrivateCAReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCertificateManagerPrivateCAReadOnly` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 23 Oktober 2018, 16:57 UTC
- Waktu yang telah diedit: 17 Agustus 2020, 22:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAReadOnly`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "acm-pca:DescribeCertificateAuthority",
      "acm-pca:DescribeCertificateAuthorityAuditReport",
      "acm-pca:ListCertificateAuthorities",
      "acm-pca:GetCertificateAuthorityCsr",
      "acm-pca:GetCertificateAuthorityCertificate",
      "acm-pca:GetCertificate",
```

```
      "acm-pca:GetPolicy",
      "acm-pca:ListPermissions",
      "acm-pca:ListTags"
    ],
    "Resource" : "*"
  }
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCertificateManagerPrivateCAUser

Deskripsi: Menyediakan akses pengguna sertifikat ke AWS Certificate Manager Private Certificate Authority

`AWSCertificateManagerPrivateCAUser`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCertificateManagerPrivateCAUser` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 23 Oktober 2018, 16:53 UTC
- Waktu telah diedit: 22 Januari 2025, 15:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAUser`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCertificateManagerReadOnly

Deskripsi: Menyediakan akses baca saja ke AWS Certificate Manager (ACM).

`AWSCertificateManagerReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCertificateManagerReadOnly` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 21 Januari 2016, 17:07 UTC
- Waktu yang telah diedit: 15 Maret 2021, 16.25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerReadOnly`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "acm:DescribeCertificate",
      "acm:ListCertificates",
      "acm:GetCertificate",
      "acm:ListTagsForCertificate",
      "acm:GetAccountConfiguration"
    ],
    "Resource" : "*"
  }
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSChatbotServiceLinkedRolePolicy

Deskripsi: Peran Tertaut Layanan yang digunakan oleh AWS Chatbot.

`AWSChatbotServiceLinkedRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 18 November 2019, 16:39 UTC
- Waktu diedit: 18 November 2019, 16:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSChatbotServiceLinkedRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCleanRoomsFullAccess

Deskripsi: Memungkinkan akses penuh ke sumber daya Kamar AWS Bersih dan akses ke yang terkait Layanan AWS.

`AWSCleanRoomsFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCleanRoomsFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 12 Januari 2023, 16:10 UTC
- Waktu telah diedit: 21 Maret 2024, 15:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CleanRoomsAccess",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/*cleanrooms*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ListRolesToPickServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetRoleAndListRolePoliciesToInspectServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
```

```
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/*cleanrooms*"
    },
    {
      "Sid" : "ListPoliciesToInspectServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListPolicies"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetPolicyToInspectServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
      ],
      "Resource" : "arn:aws:iam::*:policy/*cleanrooms*"
    },
    {
      "Sid" : "ConsoleDisplayTables",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetSchema",
        "glue:GetSchemaVersion",
        "glue:BatchGetPartition"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsolePickQueryResultsBucketListAll",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "SetQueryResultsBucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucketVersions"
      ],
      "Resource" : "arn:aws:s3:::cleanrooms-queryresults*"
    },
    {
      "Sid" : "WriteQueryResults",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::cleanrooms-queryresults*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ConsoleDisplayQueryResults",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::cleanrooms-queryresults*"
    },
    {
      "Sid" : "EstablishLogDeliveries",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SetupLogGroupsDescribe",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SetupLogGroupsCreate",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/cleanrooms*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SetupLogGroupsResourcePolicy",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeResourcePolicies",
        "logs:PutResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
```

```
      }
    },
    {
      "Sid" : "ConsoleLogSummaryQueryLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:StartQuery"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/cleanrooms*"
    },
    {
      "Sid" : "ConsoleLogSummaryObtainLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:GetQueryResults"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCleanRoomsFullAccessNoQuerying

Deskripsi: Memungkinkan akses penuh ke sumber daya Kamar AWS Bersih kecuali untuk kueri dalam kolaborasi dan akses ke terkait Layanan AWS.

`AWSCleanRoomsFullAccessNoQuerying`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCleanRoomsFullAccessNoQuerying` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 12 Januari 2023, 16:12 UTC
- Waktu yang telah diedit: 14 Mei 2024, 18:31 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsFullAccessNoQuerying`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CleanRoomsAccess",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:BatchGetCollaborationAnalysisTemplate",
        "cleanrooms:BatchGetSchema",
        "cleanrooms:BatchGetSchemaAnalysisRule",
        "cleanrooms:CreateAnalysisTemplate",
        "cleanrooms:CreateCollaboration",
        "cleanrooms:CreateConfiguredTable",
        "cleanrooms:CreateConfiguredTableAnalysisRule",
        "cleanrooms:CreateConfiguredTableAssociation",
        "cleanrooms:CreateMembership",
        "cleanrooms:DeleteAnalysisTemplate",
        "cleanrooms:DeleteCollaboration",
        "cleanrooms:DeleteConfiguredTable",
        "cleanrooms:DeleteConfiguredTableAnalysisRule",
        "cleanrooms:DeleteConfiguredTableAssociation",
        "cleanrooms:DeleteMember",
        "cleanrooms:DeleteMembership",
```

```
        "cleanrooms:GetAnalysisTemplate",
        "cleanrooms:GetCollaborationAnalysisTemplate",
        "cleanrooms:GetCollaboration",
        "cleanrooms:GetConfiguredTable",
        "cleanrooms:GetConfiguredTableAnalysisRule",
        "cleanrooms:GetConfiguredTableAssociation",
        "cleanrooms:GetMembership",
        "cleanrooms:GetProtectedQuery",
        "cleanrooms:GetSchema",
        "cleanrooms:GetSchemaAnalysisRule",
        "cleanrooms:ListAnalysisTemplates",
        "cleanrooms:ListCollaborationAnalysisTemplates",
        "cleanrooms:ListCollaborations",
        "cleanrooms:ListConfiguredTableAssociations",
        "cleanrooms:ListConfiguredTables",
        "cleanrooms:ListMembers",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListProtectedQueries",
        "cleanrooms:ListSchemas",
        "cleanrooms:UpdateAnalysisTemplate",
        "cleanrooms:UpdateCollaboration",
        "cleanrooms:UpdateConfiguredTable",
        "cleanrooms:UpdateConfiguredTableAnalysisRule",
        "cleanrooms:UpdateConfiguredTableAssociation",
        "cleanrooms:UpdateMembership",
        "cleanrooms:ListTagsForResource",
        "cleanrooms:UntagResource",
        "cleanrooms:TagResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CleanRoomsNoQuerying",
      "Effect" : "Deny",
      "Action" : [
        "cleanrooms:StartProtectedQuery",
        "cleanrooms:UpdateProtectedQuery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassServiceRole",
      "Effect" : "Allow",
      "Action" : [
```

```
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/*cleanrooms*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ListRolesToPickServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetRoleAndListRolePoliciesToInspectServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/*cleanrooms*"
    },
    {
      "Sid" : "ListPoliciesToInspectServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListPolicies"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetPolicyToInspectServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
      ],
      "Resource" : "arn:aws:iam::*:policy/*cleanrooms*"
    },
```

```
    {
      "Sid" : "ConsoleDisplayTables",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetSchema",
        "glue:GetSchemaVersion",
        "glue:BatchGetPartition"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EstablishLogDeliveries",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SetupLogGroupsDescribe",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
```

```
      }
    },
    {
      "Sid" : "SetupLogGroupsCreate",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/cleanrooms*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SetupLogGroupsResourcePolicy",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeResourcePolicies",
        "logs:PutResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ConsoleLogSummaryQueryLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:StartQuery"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/cleanrooms*"
    },
    {
      "Sid" : "ConsoleLogSummaryObtainLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:GetQueryResults"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCleanRoomsMLFullAccess

Deskripsi: Memungkinkan akses penuh ke sumber daya AWS Clean Rooms dan akses ke sumber daya yang terkait Layanan AWS.

`AWSCleanRoomsMLFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCleanRoomsMLFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 November 2023, 21:02 UTC
- Waktu yang telah diedit: 10 Januari 2025, 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsMLFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CleanRoomsMLFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms-ml:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/cleanrooms-ml*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "cleanrooms-ml.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CleanRoomsConsoleNavigation",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:GetCollaboration",
        "cleanrooms: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" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCleanRoomsMLReadOnlyAccess

Deskripsi: Memungkinkan akses hanya-baca ke sumber daya AWS Clean Rooms dan akses hanya-baca ke sumber daya Kamar Bersih terkait AWS

`AWSCleanRoomsMLReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCleanRoomsMLReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 November 2023, 20:55 UTC
- Waktu telah diedit: 10 Januari 2025, 20:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsMLReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CleanRoomsConsoleNavigation",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:GetCollaboration",
        "cleanrooms:GetConfiguredAudienceModelAssociation",
        "cleanrooms:GetMembership",
        "cleanrooms:ListAnalysisTemplates",
        "cleanrooms:ListCollaborationAnalysisTemplates",
        "cleanrooms:ListCollaborationConfiguredAudienceModelAssociations",
        "cleanrooms:ListCollaborations",
        "cleanrooms:ListConfiguredTableAssociations",
        "cleanrooms:ListConfiguredTables",
        "cleanrooms:ListMembers",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListProtectedQueries",
        "cleanrooms:ListSchemas",
        "cleanrooms:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CleanRoomsMLRead",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms-ml:Get*",
        "cleanrooms-ml:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassCleanRoomsResources",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:PassMembership",
        "cleanrooms:PassCollaboration"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCleanRoomsReadOnlyAccess

Deskripsi: Mengizinkan akses hanya-baca ke sumber daya Ruang AWS Bersih dan akses hanya-baca ke sumber daya Glue AWS dan Amazon Logs terkait. CloudWatch

`AWSCleanRoomsReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCleanRoomsReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 12 Januari 2023, 16:10 UTC
- Waktu telah diedit: 12 Januari 2023, 16:10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
  "Statement" : [
    {
      "Sid" : "CleanRoomsRead",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:BatchGet*",
        "cleanrooms:Get*",
        "cleanrooms:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleDisplayTables",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetSchema",
        "glue:GetSchemaVersion",
        "glue:BatchGetPartition"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleLogSummaryQueryLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:StartQuery"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/cleanrooms*"
    },
    {
      "Sid" : "ConsoleLogSummaryObtainLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:GetQueryResults"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCloud9Administrator

Deskripsi: Menyediakan akses administrator ke AWS Cloud9.

`AWSCloud9Administrator`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCloud9Administrator` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 November 2017, 16:17 UTC
- Waktu telah diedit: 11 Oktober 2023, 12:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloud9Administrator`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloud9:*",
        "iam:GetUser",
        "iam:ListUsers",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "cloud9.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession",
        "ssm:GetConnectionStatus"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ssm:resourceTag/aws:cloud9:environment" : "*"
        },
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloud9.amazonaws.com"
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCloud9EnvironmentMember

Deskripsi: Memberikan kemampuan untuk diundang ke lingkungan pengembangan AWS bersama Cloud9.

`AWSCloud9EnvironmentMember`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCloud9EnvironmentMember` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 November 2017, 16:18 UTC
- Waktu telah diedit: 27 Januari 2025, 10:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloud9EnvironmentMember`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCloud9ServiceRolePolicy

Deskripsi: Kebijakan Peran Tertaut Layanan untuk AWS Cloud9

`AWSCloud9ServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 30 November 2017, 13:44 UTC
- Waktu yang telah diedit: 17 Januari 2022, 14.06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCloud9ServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "cloudformation:CreateStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances",
        "ec2:DeleteSecurityGroup",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DeleteStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/aws-cloud9-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/Name" : "aws-cloud9-*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-name" : "aws-cloud9-*"
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "Resource" : [
        "arn:aws:license-manager:*:*:license-configuration:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListInstanceProfiles",
        "iam:GetInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/cloud9/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AWSCloud9SSMAccessRole"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM

- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCloud9SSMInstanceProfile

Deskripsi: Kebijakan ini akan digunakan untuk melampirkan peran yang memungkinkan Cloud9 menggunakan Pengelola Sesi SSM untuk terhubung ke instans InstanceProfile

`AWSCloud9SSMInstanceProfile`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCloud9SSMInstanceProfile` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 14 Mei 2020, 11:40 UTC
- Waktu yang telah diedit: 14 Mei 2020, 11:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloud9SSMInstanceProfile`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel",
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCloud9User

Deskripsi: Memberikan izin untuk membuat lingkungan pengembangan AWS Cloud9 dan mengelola lingkungan yang dimiliki.

`AWSCloud9User`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCloud9User` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 November 2017, 16:16 UTC
- Waktu telah diedit: 27 Januari 2025, 10:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloud9User`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCloudFormationFullAccess

Deskripsi: Menyediakan akses penuh ke AWS CloudFormation.

`AWSCloudFormationFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCloudFormationFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 26 Juli 2019, 21:50 UTC
- Waktu yang telah diedit: 26 Juli 2019, 21:50 UTC

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

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCloudFormationReadOnlyAccess

Deskripsi: Menyediakan akses ke AWS CloudFormation melalui AWS Management Console.

`AWSCloudFormationReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCloudFormationReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:39 UTC
- Waktu yang telah diedit: 13 November 2019, 17:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudFormationReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCloudFrontLogger

Deskripsi: Memberikan izin menulis CloudFront Logger ke Log. CloudWatch

`AWSCloudFrontLogger`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 12 Juni 2018, 20:15 UTC
- Waktu yang telah diedit: 22 November 2019, 19:33 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCloudFrontLogger`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/cloudfront/*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCloudFrontVPCOriginServiceRolePolicy

Deskripsi: Memungkinkan CloudFront untuk mengelola Antarmuka Jaringan EC2 Elastis dan Grup Keamanan atas nama Anda.

`AWSCloudFrontVPCOriginServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 24 Oktober 2024, 17:45 UTC
- Waktu yang telah diedit: 24 Oktober 2024, 17:45 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCloudFrontVPCOriginServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCloudHSMFullAccess

Deskripsi: Menyediakan akses penuh ke semua sumber daya CloudHSM.

`AWSCloudHSMFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCloudHSMFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:39 UTC
- Waktu telah diedit: 06 Februari 2015, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudHSMFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCloudHSMReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke semua sumber daya CloudHSM.

`AWSCloudHSMReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCloudHSMReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:39 UTC
- Waktu telah diedit: 06 Februari 2015, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudHSMReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      "Effect" : "Allow",
      "Action" : [
        "cloudhsm:Get*",
        "cloudhsm:List*",
        "cloudhsm:Describe*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCloudHSMRole

Deskripsi: Kebijakan default untuk peran layanan AWS CloudHSM.

`AWSCloudHSMRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCloudHSMRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu telah diedit: 06 Februari 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCloudHSMRole`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:CreateTags",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DetachNetworkInterface"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCloudMapDiscoverInstanceAccess

Deskripsi: Menyediakan akses ke API penemuan AWS Cloud Peta.

`AWSCloudMapDiscoverInstanceAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCloudMapDiscoverInstanceAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 November 2018, 00:02 UTC
- Waktu telah diedit: 20 September 2023, 21:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapDiscoverInstanceAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCloudMapFullAccess

Deskripsi: Menyediakan akses penuh ke semua tindakan AWS Cloud Peta.

`AWSCloudMapFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCloudMapFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 November 2018, 23:57 UTC
- Waktu yang telah diedit: 29 Juli 2020, 19:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
        "route53:ListHostedZonesByName",
        "route53:CreateHostedZone",
        "route53:DeleteHostedZone",
        "route53:ChangeResourceRecordSets",
        "route53:CreateHealthCheck",
        "route53:GetHealthCheck",
        "route53:DeleteHealthCheck",
        "route53:UpdateHealthCheck",
        "ec2:DescribeVpcs",
        "ec2:DescribeRegions",
        "ec2:DescribeInstances",
        "servicediscovery:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCloudMapReadOnlyAccess

Deskripsi: Menyediakan akses hanya-baca ke semua tindakan AWS Cloud Peta.

`AWSCloudMapReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCloudMapReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 November 2018, 23:45 UTC
- Waktu telah diedit: 20 September 2023, 21:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCloudMapRegisterInstanceAccess

Deskripsi: Menyediakan akses tingkat pendaftar ke tindakan AWS Cloud Peta.

`AWSCloudMapRegisterInstanceAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCloudMapRegisterInstanceAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 November 2018, 00:04 UTC
- Waktu yang telah diedit: 20 September 2023, 21:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapRegisterInstanceAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
        "route53:ListHostedZonesByName",
```

```
        "route53:ChangeResourceRecordSets",
        "route53:CreateHealthCheck",
        "route53:GetHealthCheck",
        "route53:DeleteHealthCheck",
        "route53:UpdateHealthCheck",
        "servicediscovery:Get*",
        "servicediscovery:List*",
        "servicediscovery:RegisterInstance",
        "servicediscovery:DeregisterInstance",
        "servicediscovery:DiscoverInstances",
        "servicediscovery:DiscoverInstancesRevision",
        "ec2:DescribeInstances"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCloudShellFullAccess

Deskripsi: Hibah menggunakan AWS CloudShell dengan semua fitur

`AWSCloudShellFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCloudShellFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 15 Desember 2020, 18:07 UTC
- Waktu yang telah diedit: 15 Desember 2020, 18:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudShellFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCloudTrail_FullAccess

Deskripsi: Menyediakan akses penuh ke AWS CloudTrail.

`AWSCloudTrail_FullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCloudTrail_FullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 08 Oktober 2020, 23:41 UTC
- Waktu yang telah diedit: 22 Februari 2021, 19:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudTrail_FullAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:AddPermission",
        "sns:CreateTopic",
        "sns:SetTopicAttributes",
        "sns:GetTopicAttributes"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:aws-cloudtrail-logs*"
      ]
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutBucketPolicy",
        "s3:PutBucketPublicAccessBlock"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-cloudtrail-logs*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation",
        "s3:GetBucketPolicy"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudtrail:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:aws-cloudtrail-logs*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "iam:GetRolePolicy",
```

```
        "iam:GetUser"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "cloudtrail.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateKey",
        "kms:CreateAlias",
        "kms:ListKeys",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListGlobalTables",
        "dynamodb:ListTables"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCloudTrail_ReadOnlyAccess

Deskripsi: Menyediakan akses hanya baca ke AWS CloudTrail.

`AWSCloudTrail_ReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCloudTrail_ReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 14 Juni 2022, 17:19 UTC
- Waktu yang telah diedit: 14 Juni 2022, 17.19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudTrail_ReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:Get*",
        "cloudtrail:Describe*",
        "cloudtrail:List*",
        "cloudtrail:LookupEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy

Deskripsi: Kebijakan ini digunakan oleh peran terkait layanan bernama. AWSServiceRoleForCloudWatchAlarms_ActionSSMIncidents CloudWatch menggunakan peran terkait layanan ini untuk melakukan tindakan Manajer Insiden Manajer AWS Sistem saat CloudWatch alarm masuk ke status ALARM. Kebijakan ini memberikan izin untuk memulai insiden atas nama Anda.

`AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan

- Waktu pembuatan: 27 April 2021, 13:30 UTC
- Waktu yang telah diedit: 27 April 2021, 13:30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "StartIncidentPermissions",
      "Effect" : "Allow",
      "Action" : "ssm-incidents:StartIncident",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCodeArtifactAdminAccess

Deskripsi: Menyediakan akses penuh ke AWS CodeArtifact melalui AWS Management Console.

`AWSCodeArtifactAdminAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCodeArtifactAdminAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 16 Juni 2020, 23:53 UTC
- Waktu yang telah diedit: 16 Juni 2020, 23:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeArtifactAdminAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codeartifact:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "sts:GetServiceBearerToken",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "sts:AWSServiceName" : "codeartifact.amazonaws.com"
        }
      }
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCodeArtifactReadOnlyAccess

Deskripsi: Menyediakan akses hanya baca AWS CodeArtifact melalui AWS Management Console.

`AWSCodeArtifactReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCodeArtifactReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 25 Juni 2020, 21:23 UTC
- Waktu yang telah diedit: 25 Juni 2020, 21:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeArtifactReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codeartifact:Describe*",
        "codeartifact:Get*",
        "codeartifact:List*",
        "codeartifact:ReadFromRepository"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "sts:GetServiceBearerToken",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "sts:AWSServiceName" : "codeartifact.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCodeBuildAdminAccess

Deskripsi: Menyediakan akses penuh ke AWS CodeBuild melalui AWS Management Console. Juga lampirkan AmazonS3 ReadOnlyAccess untuk menyediakan akses untuk mengunduh artefak build, dan lampirkan IAMFull Access untuk membuat dan mengelola peran layanan. CodeBuild

`AWSCodeBuildAdminAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCodeBuildAdminAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Desember 2016, 19:04 UTC
- Waktu yang telah diedit: 16 Desember 2024, 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeBuildAdminAccess`

Versi kebijakan

Versi kebijakan: v15 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSServicesAccess",
      "Action" : [
        "codebuild:*",
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetRepository",
        "codecommit:ListBranches",
```

```
        "codecommit:ListRepositories",
        "cloudwatch:GetMetricStatistics",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "elasticfilesystem:DescribeFileSystems",
        "events:DeleteRule",
        "events:DescribeRule",
        "events:DisableRule",
        "events:EnableRule",
        "events:ListTargetsByRule",
        "events:ListRuleNamesByTarget",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets",
        "logs:GetLogEvents",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "CWLDeleteLogGroupAccess",
      "Action" : [
        "logs:DeleteLogGroup"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/codebuild/*:log-stream:*"
    },
    {
      "Sid" : "SSMParameterWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/CodeBuild/*"
    },
    {
      "Sid" : "SSMStartSessionAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ssm:StartSession"
      ],
      "Resource" : "arn:aws:ecs:*:*:task/*/*"
    },
    {
      "Sid" : "CodeStarConnectionsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:CreateConnection",
        "codestar-connections:DeleteConnection",
        "codestar-connections:UpdateConnectionInstallation",
        "codestar-connections:TagResource",
        "codestar-connections:UntagResource",
        "codestar-connections:ListConnections",
        "codestar-connections:ListInstallationTargets",
        "codestar-connections:ListTagsForResource",
        "codestar-connections:GetConnection",
        "codestar-connections:GetIndividualAccessToken",
        "codestar-connections:GetInstallationUrl",
        "codestar-connections:PassConnection",
        "codestar-connections:StartOAuthHandshake",
        "codestar-connections:UseConnection"
      ],
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "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" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCodeBuildDeveloperAccess

Deskripsi: Menyediakan akses ke AWS CodeBuild via AWS Management Console, tetapi tidak mengizinkan administrasi CodeBuild proyek. Juga lampirkan AmazonS3 ReadOnlyAccess untuk menyediakan akses untuk mengunduh artefak build.

`AWSCodeBuildDeveloperAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCodeBuildDeveloperAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Desember 2016, 19:02 UTC
- Waktu yang telah diedit: 16 Desember 2024, 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeBuildDeveloperAccess`

Versi kebijakan

Versi kebijakan: v16 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Statement" : [
    {
      "Sid" : "AWSServicesAccess",
      "Action" : [
        "codebuild:StartBuild",
        "codebuild:StopBuild",
        "codebuild:StartBuildBatch",
        "codebuild:StopBuildBatch",
        "codebuild:RetryBuild",
        "codebuild:RetryBuildBatch",
        "codebuild:BatchGet*",
        "codebuild:GetResourcePolicy",
        "codebuild:DescribeTestCases",
        "codebuild:DescribeCodeCoverages",
        "codebuild:List*",
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetRepository",
        "codecommit:ListBranches",
        "cloudwatch:GetMetricStatistics",
        "events:DescribeRule",
        "events:ListTargetsByRule",
        "events:ListRuleNamesByTarget",
        "logs:GetLogEvents",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "SSMParameterWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/CodeBuild/*"
    },
    {
      "Sid" : "SSMStartSessionAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
```

```
      "Resource" : "arn:aws:ecs:*:*:task/*/*"
    },
    {
      "Sid" : "CodeStarConnectionsUserAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:ListConnections",
        "codestar-connections:GetConnection"
      ],
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "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"
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCodeBuildReadOnlyAccess

Deskripsi: Menyediakan akses hanya baca AWS CodeBuild melalui AWS Management Console. Juga lampirkan AmazonS3 ReadOnlyAccess untuk menyediakan akses untuk mengunduh artefak build.

`AWSCodeBuildReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCodeBuildReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Desember 2016, 19:03 UTC
- Waktu yang telah diedit: 16 Desember 2024, 19:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeBuildReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v13 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "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"
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCodeCommitFullAccess

Deskripsi: Menyediakan akses penuh ke AWS CodeCommit melalui AWS Management Console.

`AWSCodeCommitFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCodeCommitFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 09 Juli 2015, 17:02 UTC
- Waktu yang telah diedit: 10 Januari 2025, 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeCommitFullAccess`

Versi kebijakan

Versi kebijakan: v11 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
    },
    {
      "Sid" : "CloudWatchEventsCodeCommitRulesAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:DisableRule",
        "events:EnableRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/codecommit*"
    },
    {
      "Sid" : "SNSTopicAndSubscriptionAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:DeleteTopic",
        "sns:Subscribe",
        "sns:Unsubscribe",
        "sns:SetTopicAttributes"
      ],
      "Resource" : "arn:aws:sns:*:*:codecommit*"
    },
    {
      "Sid" : "SNSTopicAndSubscriptionReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics",
        "sns:ListSubscriptionsByTopic",
        "sns:GetTopicAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LambdaReadOnlyListAccess",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "IAMReadOnlyListAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListUsers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMReadOnlyConsoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListAccessKeys",
        "iam:ListSSHPublicKeys",
        "iam:ListServiceSpecificCredentials"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    },
    {
      "Sid" : "IAMUserSSHKeys",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteSSHPublicKey",
        "iam:GetSSHPublicKey",
        "iam:ListSSHPublicKeys",
        "iam:UpdateSSHPublicKey",
        "iam:UploadSSHPublicKey"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    },
    {
      "Sid" : "IAMSelfManageServiceSpecificCredentials",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceSpecificCredential",
        "iam:UpdateServiceSpecificCredential",
        "iam:DeleteServiceSpecificCredential",
        "iam:ResetServiceSpecificCredential"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    },
    {
```

```
      "Sid" : "CodeStarNotificationsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:CreateNotificationRule",
        "codestar-notifications:DescribeNotificationRule",
        "codestar-notifications:UpdateNotificationRule",
        "codestar-notifications:DeleteNotificationRule",
        "codestar-notifications:Subscribe",
        "codestar-notifications:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "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/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCodeCommitPowerUser

Deskripsi: Menyediakan akses penuh ke AWS CodeCommit repositori, tetapi tidak mengizinkan penghapusan repositori.

`AWSCodeCommitPowerUser`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCodeCommitPowerUser` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 09 Juli 2015, 17:06 UTC
- Waktu telah diedit: 10 Januari 2025, 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeCommitPowerUser`

Versi kebijakan

Versi kebijakan: v16 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codecommit:AssociateApprovalRuleTemplateWithRepository",
        "codecommit:BatchAssociateApprovalRuleTemplateWithRepositories",
        "codecommit:BatchDisassociateApprovalRuleTemplateFromRepositories",
        "codecommit:BatchGet*",
        "codecommit:BatchDescribe*",
        "codecommit:Create*",
        "codecommit:DeleteBranch",
        "codecommit:DeleteFile",
        "codecommit:Describe*",
        "codecommit:DisassociateApprovalRuleTemplateFromRepository",
        "codecommit:EvaluatePullRequestApprovalRules",
        "codecommit:Get*",
        "codecommit:List*",
        "codecommit:Merge*",
        "codecommit:OverridePullRequestApprovalRules",
        "codecommit:Put*",
        "codecommit:Post*",
        "codecommit:TagResource",
        "codecommit:Test*",
        "codecommit:UntagResource",
        "codecommit:Update*",
        "codecommit:GitPull",
        "codecommit:GitPush"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "CloudWatchEventsCodeCommitRulesAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:DisableRule",
        "events:EnableRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/codecommit*"
    },
    {
      "Sid" : "SNSTopicAndSubscriptionAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:Subscribe",
        "sns:Unsubscribe"
      ],
      "Resource" : "arn:aws:sns:*:*:codecommit*"
    },
    {
      "Sid" : "SNSTopicAndSubscriptionReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics",
        "sns:ListSubscriptionsByTopic",
        "sns:GetTopicAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LambdaReadOnlyListAccess",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMReadOnlyListAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:ListUsers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMReadOnlyConsoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListAccessKeys",
        "iam:ListSSHPublicKeys",
        "iam:ListServiceSpecificCredentials"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    },
    {
      "Sid" : "IAMUserSSHKeys",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteSSHPublicKey",
        "iam:GetSSHPublicKey",
        "iam:ListSSHPublicKeys",
        "iam:UpdateSSHPublicKey",
        "iam:UploadSSHPublicKey"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    },
    {
      "Sid" : "IAMSelfManageServiceSpecificCredentials",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceSpecificCredential",
        "iam:UpdateServiceSpecificCredential",
        "iam:DeleteServiceSpecificCredential",
        "iam:ResetServiceSpecificCredential"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    },
    {
      "Sid" : "CodeStarNotificationsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:CreateNotificationRule",
        "codestar-notifications:DescribeNotificationRule",
```

```
        "codestar-notifications:UpdateNotificationRule",
        "codestar-notifications:Subscribe",
        "codestar-notifications:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "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/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCodeCommitReadOnly

Deskripsi: Menyediakan akses hanya baca AWS CodeCommit melalui AWS Management Console.

`AWSCodeCommitReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCodeCommitReadOnly` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 09 Juli 2015, 17:05 UTC
- Waktu telah diedit: 10 Januari 2025, 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeCommitReadOnly`

Versi kebijakan

Versi kebijakan: v12 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      "Effect" : "Allow",
      "Action" : [
        "codecommit:BatchGet*",
        "codecommit:BatchDescribe*",
        "codecommit:Describe*",
        "codecommit:EvaluatePullRequestApprovalRules",
        "codecommit:Get*",
        "codecommit:List*",
        "codecommit:GitPull"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchEventsCodeCommitRulesReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/codecommit*"
    },
    {
      "Sid" : "SNSSubscriptionAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics",
        "sns:ListSubscriptionsByTopic",
        "sns:GetTopicAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LambdaReadOnlyListAccess",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMReadOnlyListAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListUsers"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMReadOnlyConsoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListSSHPublicKeys",
        "iam:ListServiceSpecificCredentials",
        "iam:ListAccessKeys",
        "iam:GetSSHPublicKey"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    },
    {
      "Sid" : "CodeStarConnectionsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:ListConnections",
        "codestar-connections:GetConnection"
      ],
      "Resource" : "arn:aws:codestar-connections:*:*:connection/*"
    },
    {
      "Sid" : "CodeStarNotificationsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:DescribeNotificationRule"
      ],
      "Resource" : "*",
      "Condition" : {
        "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" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCodeDeployDeployerAccess

Deskripsi: Menyediakan akses untuk mendaftar dan menyebarkan revisi.

`AWSCodeDeployDeployerAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCodeDeployDeployerAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 19 Mei 2015, 18:18 UTC

- Waktu telah diedit: 16 Desember 2024, 20:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployDeployerAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codedeploy:Batch*",
        "codedeploy:CreateDeployment",
        "codedeploy:Get*",
        "codedeploy:List*",
        "codedeploy:RegisterApplicationRevision"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:CreateNotificationRule",
        "codestar-notifications:DescribeNotificationRule",
        "codestar-notifications:UpdateNotificationRule",
        "codestar-notifications:Subscribe",
        "codestar-notifications:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "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" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCodeDeployFullAccess

Deskripsi: Menyediakan akses penuh ke CodeDeploy sumber daya.

`AWSCodeDeployFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCodeDeployFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 19 Mei 2015, 18:13 UTC
- Waktu telah diedit: 16 Desember 2024, 20:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployFullAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : "codedeploy:*",
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:CreateNotificationRule",
```

```
        "codestar-notifications:DescribeNotificationRule",
        "codestar-notifications:UpdateNotificationRule",
        "codestar-notifications:DeleteNotificationRule",
        "codestar-notifications:Subscribe",
        "codestar-notifications:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "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" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCodeDeployReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke CodeDeploy sumber daya.

`AWSCodeDeployReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCodeDeployReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 19 Mei 2015, 18:21 UTC
- Waktu yang telah diedit: 16 Desember 2024, 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codedeploy:Batch*",
        "codedeploy:Get*",
        "codedeploy:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsPowerUserAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:DescribeNotificationRule"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "codestar-notifications:NotificationsForResource" :
 "arn:aws:codedeploy:*:*:application:*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListEventTypes",
        "codestar-notifications:ListTargets"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCodeDeployRole

Deskripsi: Menyediakan akses CodeDeploy layanan untuk memperluas tag dan berinteraksi dengan Auto Scaling atas nama Anda.

`AWSCodeDeployRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCodeDeployRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 04 Mei 2015, 18:05 UTC
- Waktu telah diedit: 16 Agustus 2023, 20:38 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeDeployRole`

Versi kebijakan

Versi kebijakan: v11 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:CompleteLifecycleAction",
        "autoscaling:DeleteLifecycleHook",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeLifecycleHooks",
        "autoscaling:PutLifecycleHook",
        "autoscaling:RecordLifecycleActionHeartbeat",
        "autoscaling:CreateAutoScalingGroup",
        "autoscaling:CreateOrUpdateTags",
        "autoscaling:UpdateAutoScalingGroup",
        "autoscaling:EnableMetricsCollection",
        "autoscaling:DescribePolicies",
        "autoscaling:DescribeScheduledActions",
        "autoscaling:DescribeNotificationConfigurations",
        "autoscaling:SuspendProcesses",
        "autoscaling:ResumeProcesses",
        "autoscaling:AttachLoadBalancers",
        "autoscaling:AttachLoadBalancerTargetGroups",
        "autoscaling:PutScalingPolicy",
        "autoscaling:PutScheduledUpdateGroupAction",
        "autoscaling:PutNotificationConfiguration",
        "autoscaling:PutWarmPool",
        "autoscaling:DescribeScalingActivities",
        "autoscaling:DeleteAutoScalingGroup",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:TerminateInstances",
        "tag:GetResources",
        "sns:Publish",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:PutMetricAlarm",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
```

```
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:DeregisterTargets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCodeDeployRoleForCloudFormation

Deskripsi: Menyediakan akses CodeDeploy layanan untuk memanggil fungsi Lambda atas nama Anda untuk melakukan penyebaran biru/hijau melalui. CloudFormation

`AWSCodeDeployRoleForCloudFormation`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCodeDeployRoleForCloudFormation` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 19 Mei 2020, 17:12 UTC
- Waktu yang telah diedit: 19 Mei 2020, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForCloudFormation`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:CodeDeployHook_*",
      "Effect" : "Allow"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCodeDeployRoleForECS

Deskripsi: Menyediakan CodeDeploy layanan akses luas untuk melakukan penyebaran biru/hijau ECS atas nama Anda. Memberikan akses penuh ke layanan dukungan, seperti akses penuh untuk membaca semua objek S3, memanggil semua fungsi Lambda, mempublikasikan ke semua topik SNS dalam akun dan memperbarui semua layanan ECS.

`AWSCodeDeployRoleForECS`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCodeDeployRoleForECS` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 November 2018, 20:40 UTC
- Waktu yang telah diedit: 23 September 2019, 22:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployRoleForECS`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ecs:DescribeServices",
        "ecs:CreateTaskSet",
        "ecs:UpdateServicePrimaryTaskSet",
        "ecs:DeleteTaskSet",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:ModifyListener",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:ModifyRule",
        "lambda:InvokeFunction",
        "cloudwatch:DescribeAlarms",
        "sns:Publish",
        "s3:GetObject",
```

```
        "s3:GetObjectVersion"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "ecs-tasks.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCodeDeployRoleForECSLimited

Deskripsi: Menyediakan CodeDeploy layanan akses terbatas untuk melakukan penyebaran biru/hijau ECS atas nama Anda.

`AWSCodeDeployRoleForECSLimited`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCodeDeployRoleForECSLimited` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 November 2018, 20:42 UTC
- Waktu yang telah diedit: 23 September 2019, 22:10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployRoleForECSLimited`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ecs:DescribeServices",
        "ecs:CreateTaskSet",
        "ecs:UpdateServicePrimaryTaskSet",
        "ecs:DeleteTaskSet",
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : "arn:aws:sns:*:*:CodeDeployTopic_*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
```

```
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:ModifyListener",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:ModifyRule"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:CodeDeployHook_*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "s3:ExistingObjectTag/UseWithCodeDeploy" : "true"
        }
      },
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/ecsTaskExecutionRole",
        "arn:aws:iam::*:role/ECSTaskExecution*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "ecs-tasks.amazonaws.com"
          ]
        }
```

```
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCodeDeployRoleForLambda

Deskripsi: Menyediakan akses CodeDeploy layanan untuk melakukan penyebaran Lambda atas nama Anda.

`AWSCodeDeployRoleForLambda`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCodeDeployRoleForLambda` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 28 November 2017, 14:05 UTC
- Waktu yang telah diedit: 03 Desember 2019, 19:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForLambda`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "lambda:UpdateAlias",
        "lambda:GetAlias",
        "lambda:GetProvisionedConcurrencyConfig",
        "sns:Publish"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::*/CodeDeploy/*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "s3:ExistingObjectTag/UseWithCodeDeploy" : "true"
        }
      },
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:CodeDeployHook_*",
      "Effect" : "Allow"
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCodeDeployRoleForLambdaLimited

Deskripsi: Menyediakan akses terbatas CodeDeploy layanan untuk melakukan penyebaran Lambda atas nama Anda.

`AWSCodeDeployRoleForLambdaLimited`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCodeDeployRoleForLambdaLimited` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 17 Agustus 2020, 17:14 UTC
- Waktu yang telah diedit: 17 Agustus 2020, 17:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForLambdaLimited`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "lambda:UpdateAlias",
        "lambda:GetAlias",
        "lambda:GetProvisionedConcurrencyConfig"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::*/CodeDeploy/*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "s3:ExistingObjectTag/UseWithCodeDeploy" : "true"
        }
      },
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "lambda:InvokeFunction"
```

```
      ],
      "Resource" : "arn:aws:lambda:*:*:function:CodeDeployHook_*",
      "Effect" : "Allow"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCodePipeline_FullAccess

Deskripsi: Menyediakan akses penuh ke AWS CodePipeline melalui AWS Management Console.

`AWSCodePipeline_FullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCodePipeline_FullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 Agustus 2020, 22:38 UTC
- Waktu yang telah diedit: 14 Maret 2024, 17:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodePipeline_FullAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Statement" : [
    {
      "Action" : [
        "codepipeline:*",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks",
        "cloudformation:ListChangeSets",
        "cloudtrail:DescribeTrails",
        "codebuild:BatchGetProjects",
        "codebuild:CreateProject",
        "codebuild:ListCuratedEnvironmentImages",
        "codebuild:ListProjects",
        "codecommit:ListBranches",
        "codecommit:GetReferences",
        "codecommit:ListRepositories",
        "codedeploy:BatchGetDeploymentGroups",
        "codedeploy:ListApplications",
        "codedeploy:ListDeploymentGroups",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "ecs:ListClusters",
        "ecs:ListServices",
        "elasticbeanstalk:DescribeApplications",
        "elasticbeanstalk:DescribeEnvironments",
        "iam:ListRoles",
        "iam:GetRole",
        "lambda:ListFunctions",
        "events:ListRules",
        "events:ListTargetsByRule",
        "events:DescribeRule",
        "opsworks:DescribeApps",
        "opsworks:DescribeLayers",
        "opsworks:DescribeStacks",
        "s3:ListAllMyBuckets",
        "sns:ListTopics",
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListTargets",
```

```
        "codestar-notifications:ListTagsforResource",
        "codestar-notifications:ListEventTypes",
        "states:ListStateMachines"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Sid" : "CodePipelineAuthoringAccess"
    },
    {
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket",
        "s3:GetBucketPolicy",
        "s3:GetBucketVersioning",
        "s3:GetObjectVersion",
        "s3:CreateBucket",
        "s3:PutBucketPolicy"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:s3::*:codepipeline-*",
      "Sid" : "CodePipelineArtifactsReadWriteAccess"
    },
    {
      "Action" : [
        "cloudtrail:PutEventSelectors",
        "cloudtrail:CreateTrail",
        "cloudtrail:GetEventSelectors",
        "cloudtrail:StartLogging"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:cloudtrail:*:*:trail/codepipeline-source-trail",
      "Sid" : "CodePipelineSourceTrailReadWriteAccess"
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/cwe-role-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
```

```
            "events.amazonaws.com"
          ]
        }
      },
      "Sid" : "EventsIAMPassRole"
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "codepipeline.amazonaws.com"
          ]
        }
      },
      "Sid" : "CodePipelineIAMPassRole"
    },
    {
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:DeleteRule",
        "events:DisableRule",
        "events:RemoveTargets"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:events:*:*:rule/codepipeline-*"
      ],
      "Sid" : "CodePipelineEventsReadWriteAccess"
    },
    {
      "Sid" : "CodeStarNotificationsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:CreateNotificationRule",
        "codestar-notifications:DescribeNotificationRule",
        "codestar-notifications:UpdateNotificationRule",
        "codestar-notifications:DeleteNotificationRule",
        "codestar-notifications:Subscribe",
```

```
        "codestar-notifications:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "codestar-notifications:NotificationsForResource" : "arn:aws:codepipeline:*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsSNSTopicCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:SetTopicAttributes"
      ],
      "Resource" : "arn:aws:sns:*:*:codestar-notifications*"
    },
    {
      "Sid" : "CodeStarNotificationsChatbotAccess",
      "Effect" : "Allow",
      "Action" : [
        "chatbot:DescribeSlackChannelConfigurations",
        "chatbot:ListMicrosoftTeamsChannelConfigurations"
      ],
      "Resource" : "*"
    }
  ],
  "Version" : "2012-10-17"
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCodePipeline_ReadOnlyAccess

Deskripsi: Menyediakan akses hanya baca AWS CodePipeline melalui AWS Management Console.

`AWSCodePipeline_ReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCodePipeline_ReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 Agustus 2020, 22:25 UTC
- Waktu yang telah diedit: 03 Agustus 2020, 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodePipeline_ReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Statement" : [
    {
      "Action" : [
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:GetPipelineExecution",
        "codepipeline:ListPipelineExecutions",
        "codepipeline:ListActionExecutions",
        "codepipeline:ListActionTypes",
        "codepipeline:ListPipelines",
        "codepipeline:ListTagsForResource",
        "s3:ListAllMyBuckets",
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListEventTypes",
```

```
        "codestar-notifications:ListTargets"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket",
        "s3:GetBucketPolicy"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:s3::*:codepipeline-*"
    },
    {
      "Sid" : "CodeStarNotificationsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:DescribeNotificationRule"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "codestar-notifications:NotificationsForResource" : "arn:aws:codepipeline:*"
        }
      }
    }
  ],
  "Version" : "2012-10-17"
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCodePipelineApproverAccess

Deskripsi: Menyediakan akses untuk melihat dan menyetujui perubahan manual untuk semua saluran pipa

`AWSCodePipelineApproverAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCodePipelineApproverAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 Juli 2016, 18:59 UTC
- Waktu telah diedit: 02 Agustus 2017, 17:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodePipelineApproverAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:GetPipelineExecution",
        "codepipeline:ListPipelineExecutions",
        "codepipeline:ListPipelines",
```

```
        "codepipeline:PutApprovalResult"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCodePipelineCustomActionAccess

Deskripsi: Menyediakan akses untuk tindakan kustom untuk polling untuk rincian pekerjaan (termasuk kredenal sementara) dan melaporkan pembaruan status ke. AWS CodePipeline

`AWSCodePipelineCustomActionAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCodePipelineCustomActionAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 09 Juli 2015, 17:02 UTC
- Waktu telah diedit: 09 Juli 2015, 17:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodePipelineCustomActionAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Statement" : [
    {
      "Action" : [
        "codepipeline:AcknowledgeJob",
        "codepipeline:GetJobDetails",
        "codepipeline:PollForJobs",
        "codepipeline:PutJobFailureResult",
        "codepipeline:PutJobSuccessResult"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ],
  "Version" : "2012-10-17"
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCodeStarFullAccess

Deskripsi: Menyediakan akses penuh ke AWS CodeStar melalui AWS Management Console.

`AWSCodeStarFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCodeStarFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 19 April 2017, 16:23 UTC
- Waktu telah diedit: 28 Maret 2023, 00:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeStarFullAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CodeStarEC2",
      "Effect" : "Allow",
      "Action" : [
        "codestar:*",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "cloud9:DescribeEnvironment*",
        "cloud9:ValidateEnvironmentName"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarCF",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStack*",
        "cloudformation:ListStacks*",
        "cloudformation:GetTemplateSummary"
```

```
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awscodestar-*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCodeStarNotificationsServiceRolePolicy

Deskripsi: Memungkinkan AWS CodeStar Pemberitahuan untuk mengakses CloudWatch Acara Amazon atas nama Anda

`AWSCodeStarNotificationsServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 05 November 2019, 16:10 UTC
- Waktu yang telah diedit: 19 Maret 2020, 16:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCodeStarNotificationsServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCodeStarServiceRole

Deskripsi: JANGAN GUNAKAN - Kebijakan Peran AWS CodeStar Layanan yang memberikan hak administratif CodeStar untuk mengelola IAM dan sumber daya layanan lainnya atas nama pelanggan.

`AWSCodeStarServiceRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCodeStarServiceRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 19 April 2017, 15:20 UTC
- Waktu yang telah diedit: 20 September 2021 19:11 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeStarServiceRole`

Versi kebijakan

Versi kebijakan: v11 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ProjectEventRules",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:RemoveTargets",
        "events:PutRule",
        "events:DeleteRule",
        "events:DescribeRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/awscodestar-*"
      ]
    },
    {
      "Sid" : "ProjectStack",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:*Stack*",
        "cloudformation:CreateChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:GetTemplate"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awscodestar-*",
        "arn:aws:cloudformation:*:*:stack/awseb-*",
        "arn:aws:cloudformation:*:*:stack/aws-cloud9-*",
        "arn:aws:cloudformation:*:aws:transform/CodeStar*"
      ]
    },
    {
      "Sid" : "ProjectStackTemplate",
      "Effect" : "Allow",
```

```
      "Action" : [
        "cloudformation:GetTemplateSummary",
        "cloudformation:DescribeChangeSet"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ProjectQuickstarts",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::awscodestar-*/*"
      ]
    },
    {
      "Sid" : "ProjectS3Buckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:*"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-codestar-*",
        "arn:aws:s3:::elasticbeanstalk-*"
      ]
    },
    {
      "Sid" : "ProjectServices",
      "Effect" : "Allow",
      "Action" : [
        "codestar:*",
        "codecommit:*",
        "codepipeline:*",
        "codedeploy:*",
        "codebuild:*",
        "autoscaling:*",
        "cloudwatch:Put*",
        "ec2:*",
        "elasticbeanstalk:*",
        "elasticloadbalancing:*",
        "iam:ListRoles",
        "logs:*",
        "sns:*",
```

```
        "cloud9:CreateEnvironmentEC2",
        "cloud9:DeleteEnvironment",
        "cloud9:DescribeEnvironment*",
        "cloud9:ListEnvironments"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ProjectWorkerRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:GetRole",
        "iam:PassRole",
        "iam:GetRolePolicy",
        "iam:PutRolePolicy",
        "iam:SetDefaultPolicyVersion",
        "iam:CreatePolicy",
        "iam:DeletePolicy",
        "iam:AddRoleToInstanceProfile",
        "iam:CreateInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/CodeStarWorker*",
        "arn:aws:iam::*:policy/CodeStarWorker*",
        "arn:aws:iam::*:instance-profile/awscodestar-*"
      ]
    },
    {
      "Sid" : "ProjectTeamMembers",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachUserPolicy",
        "iam:DetachUserPolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnEquals" : {
```

```
          "iam:PolicyArn" : [
            "arn:aws:iam::*:policy/CodeStar_*"
          ]
        }
      }
    },
    {
      "Sid" : "ProjectRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreatePolicy",
        "iam:DeletePolicy",
        "iam:CreatePolicyVersion",
        "iam:DeletePolicyVersion",
        "iam:ListEntitiesForPolicy",
        "iam:ListPolicyVersions",
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
      ],
      "Resource" : [
        "arn:aws:iam::*:policy/CodeStar_*"
      ]
    },
    {
      "Sid" : "InspectServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-codestar-service-role",
        "arn:aws:iam::*:role/service-role/aws-codestar-service-role"
      ]
    },
    {
      "Sid" : "IAMLinkRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "cloud9.amazonaws.com"
```

```
        }
      }
    },
    {
      "Sid" : "DescribeConfigRuleForARN",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigRules"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ProjectCodeStarConnections",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection",
        "codestar-connections:GetConnection"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ProjectCodeStarConnectionsPassConnections",
      "Effect" : "Allow",
      "Action" : "codestar-connections:PassConnection",
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "codestar-connections:PassedToService" : "codepipeline.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCompromisedKeyQuarantine

Deskripsi: Menolak akses ke tindakan tertentu, yang diterapkan oleh AWS tim jika kredensi pengguna IAM telah disusupi atau diekspos secara publik. Jangan hapus kebijakan ini. Sebagai gantinya, ikuti instruksi yang ditentukan dalam email yang dikirimkan kepada Anda mengenai acara ini.

`AWSCompromisedKeyQuarantine`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCompromisedKeyQuarantine` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 11 Agustus 2020, 18:04 UTC
- Waktu yang telah diedit: 11 Agustus 2020, 18:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCompromisedKeyQuarantine`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Deny",
      "Action" : [
        "iam:AttachGroupPolicy",
        "iam:AttachRolePolicy",
```

```
        "iam:AttachUserPolicy",
        "iam:ChangePassword",
        "iam:CreateAccessKey",
        "iam:CreateInstanceProfile",
        "iam:CreateLoginProfile",
        "iam:CreateRole",
        "iam:CreateUser",
        "iam:DetachUserPolicy",
        "iam:PutUserPermissionsBoundary",
        "iam:PutUserPolicy",
        "iam:UpdateAccessKey",
        "iam:UpdateAccountPasswordPolicy",
        "iam:UpdateUser",
        "ec2:RequestSpotInstances",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "organizations:CreateAccount",
        "organizations:CreateOrganization",
        "organizations:InviteAccountToOrganization",
        "lambda:CreateFunction",
        "lightsail:Create*",
        "lightsail:Start*",
        "lightsail:Delete*",
        "lightsail:Update*",
        "lightsail:GetInstanceAccessDetails",
        "lightsail:DownloadDefaultKeyPair"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCompromisedKeyQuarantineV2

Deskripsi: Menolak akses ke tindakan tertentu, yang diterapkan oleh AWS tim jika kredensi pengguna IAM telah disusupi atau diekspos secara publik. Jangan hapus kebijakan ini. Sebagai gantinya, ikuti petunjuk yang ditentukan dalam kasus dukungan yang dibuat untuk Anda mengenai acara ini.

`AWSCompromisedKeyQuarantineV2`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCompromisedKeyQuarantineV2` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 21 April 2021, 22:30 UTC
- Waktu telah diedit: 02 Oktober 2024, 16:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCompromisedKeyQuarantineV2`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Deny",
      "Action" : [
        "cloudtrail:LookupEvents",
        "ec2:RequestSpotInstances",
        "ec2:RunInstances",
        "ec2:StartInstances",
```

```
        "iam:AddUserToGroup",
        "iam:AttachGroupPolicy",
        "iam:AttachRolePolicy",
        "iam:AttachUserPolicy",
        "iam:ChangePassword",
        "iam:CreateAccessKey",
        "iam:CreateInstanceProfile",
        "iam:CreateLoginProfile",
        "iam:CreatePolicyVersion",
        "iam:CreateRole",
        "iam:CreateUser",
        "iam:DetachUserPolicy",
        "iam:PassRole",
        "iam:PutGroupPolicy",
        "iam:PutRolePolicy",
        "iam:PutUserPermissionsBoundary",
        "iam:PutUserPolicy",
        "iam:SetDefaultPolicyVersion",
        "iam:UpdateAccessKey",
        "iam:UpdateAccountPasswordPolicy",
        "iam:UpdateAssumeRolePolicy",
        "iam:UpdateLoginProfile",
        "iam:UpdateUser",
        "lambda:AddLayerVersionPermission",
        "lambda:AddPermission",
        "lambda:CreateFunction",
        "lambda:GetPolicy",
        "lambda:ListTags",
        "lambda:PutProvisionedConcurrencyConfig",
        "lambda:TagResource",
        "lambda:UntagResource",
        "lambda:UpdateFunctionCode",
        "lightsail:Create*",
        "lightsail:Delete*",
        "lightsail:DownloadDefaultKeyPair",
        "lightsail:GetInstanceAccessDetails",
        "lightsail:Start*",
        "lightsail:Update*",
        "organizations:CreateAccount",
        "organizations:CreateOrganization",
        "organizations:InviteAccountToOrganization",
        "s3:DeleteBucket",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
```

```
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketAcl",
        "s3:PutBucketOwnershipControls",
        "s3:DeleteBucketPolicy",
        "s3:ObjectOwnerOverrideToBucketOwner",
        "s3:PutAccountPublicAccessBlock",
        "s3:PutBucketPolicy",
        "s3:ListAllMyBuckets",
        "ec2:PurchaseReservedInstancesOffering",
        "ec2:AcceptReservedInstancesExchangeQuote",
        "ec2:CreateReservedInstancesListing",
        "savingsplans:CreateSavingsPlan",
        "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" : [
        "*"
```

```
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCompromisedKeyQuarantineV3

Deskripsi: Menolak akses ke tindakan tertentu, diterapkan oleh AWS jika kredensi pengguna IAM telah disusupi atau diekspos secara publik. Kebijakan ini bertujuan untuk membatasi potensi kerusakan yang mungkin disebabkan oleh aktivitas terkait penipuan yang mengarah ke biaya yang tidak sah, sementara tidak berdampak pada sumber daya yang ada. Jangan hapus kebijakan ini. Sebagai gantinya, ikuti petunjuk yang ditentukan dalam kasus dukungan yang dibuat untuk Anda mengenai acara ini.

`AWSCompromisedKeyQuarantineV3`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCompromisedKeyQuarantineV3` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 21 Agustus 2024, 17:36 UTC
- Waktu yang telah diedit: 02 Oktober 2024, 16:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCompromisedKeyQuarantineV3`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Deny",
      "Action" : [
        "cloudtrail:LookupEvents",
        "ec2:RequestSpotInstances",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "iam:AddUserToGroup",
        "iam:AttachGroupPolicy",
        "iam:AttachRolePolicy",
        "iam:AttachUserPolicy",
        "iam:ChangePassword",
        "iam:CreateAccessKey",
        "iam:CreateInstanceProfile",
        "iam:CreateLoginProfile",
        "iam:CreatePolicyVersion",
        "iam:CreateRole",
        "iam:CreateUser",
        "iam:DetachUserPolicy",
        "iam:PassRole",
        "iam:PutGroupPolicy",
        "iam:PutRolePolicy",
        "iam:PutUserPermissionsBoundary",
        "iam:PutUserPolicy",
        "iam:SetDefaultPolicyVersion",
        "iam:UpdateAccessKey",
        "iam:UpdateAccountPasswordPolicy",
        "iam:UpdateAssumeRolePolicy",
        "iam:UpdateLoginProfile",
        "iam:UpdateUser",
```

```
        "lambda:AddLayerVersionPermission",
        "lambda:AddPermission",
        "lambda:CreateFunction",
        "lambda:GetPolicy",
        "lambda:ListTags",
        "lambda:PutProvisionedConcurrencyConfig",
        "lambda:TagResource",
        "lambda:UntagResource",
        "lambda:UpdateFunctionCode",
        "lightsail:Create*",
        "lightsail:Delete*",
        "lightsail:DownloadDefaultKeyPair",
        "lightsail:GetInstanceAccessDetails",
        "lightsail:Start*",
        "lightsail:Update*",
        "organizations:CreateAccount",
        "organizations:CreateOrganization",
        "organizations:InviteAccountToOrganization",
        "s3:DeleteBucket",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketAcl",
        "s3:PutBucketOwnershipControls",
        "s3:DeleteBucketPolicy",
        "s3:ObjectOwnerOverrideToBucketOwner",
        "s3:PutAccountPublicAccessBlock",
        "s3:PutBucketPolicy",
        "s3:ListAllMyBuckets",
        "ec2:PurchaseReservedInstancesOffering",
        "ec2:AcceptReservedInstancesExchangeQuote",
        "ec2:CreateReservedInstancesListing",
        "savingsplans:CreateSavingsPlan",
        "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" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSConfigMultiAccountSetupPolicy

Deskripsi: Mengizinkan Config memanggil AWS layanan dan menerapkan sumber daya konfigurasi di seluruh organisasi

`AWSConfigMultiAccountSetupPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 17 Juni 2019, 18:03 UTC
- Waktu telah diedit: 24 Februari 2023, 01:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSConfigMultiAccountSetupPolicy`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "config:PutConfigRule",
        "config:DeleteConfigRule"
      ],
      "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/config-
multiaccountsetup.amazonaws.com/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigurationRecorders"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeAccount"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:PutConformancePack",
        "config:DeleteConformancePack"
      ],
      "Resource" : "arn:aws:config:*:*:conformance-pack/aws-service-conformance-pack/
config-multiaccountsetup.amazonaws.com/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConformancePackStatus"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/config-conforms.amazonaws.com/
AWSServiceRoleForConfigConforms"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/config-conforms.amazonaws.com/
AWSServiceRoleForConfigConforms",
```

```
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "config-conforms.amazonaws.com"
        }
      }
    },
    {
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Effect" : "Allow",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSConfigRemediationServiceRolePolicy

Deskripsi: Memungkinkan AWS Config untuk memulihkan sumber daya yang tidak sesuai atas nama Anda.

`AWSConfigRemediationServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan

- Waktu pembuatan: 18 Juni 2019, 21:21 UTC
- Waktu yang telah diedit: 18 Juni 2019, 21:21 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSConfigRemediationServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSConfigRoleForOrganizations

Deskripsi: Memungkinkan AWS Config memanggil Organizations read-only AWS APIs

`AWSConfigRoleForOrganizations`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSConfigRoleForOrganizations` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 19 Maret 2018, 22:53 UTC
- Waktu yang telah diedit: 24 November 2020, 20:19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSConfigRoleForOrganizations`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSConfigRulesExecutionRole

Deskripsi: Mengizinkan fungsi AWS Lambda mengakses AWS Config API dan snapshot konfigurasi yang AWS diberikan Config secara berkala ke Amazon S3. Akses ini diperlukan oleh fungsi yang mengevaluasi perubahan konfigurasi untuk aturan Config kustom.

`AWSConfigRulesExecutionRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSConfigRulesExecutionRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 25 Maret 2016, 17:59 UTC
- Waktu yang telah diedit: 13 Mei 2019, 21:33 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSConfigRulesExecutionRole`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::*/AWSLogs/*/Config/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:Put*",
        "config:Get*",
        "config:List*",
        "config:Describe*",
        "config:BatchGet*",
        "config:Select*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSConfigServiceRolePolicy

Deskripsi: Mengizinkan Config memanggil AWS layanan dan mengumpulkan konfigurasi sumber daya atas nama Anda.

`AWSConfigServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 30 Mei 2018, 23:31 UTC
- Waktu yang telah diedit: 20 Juni 2025, 17:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSConfigServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v59 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSConfigServiceRolePolicyStatementID",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:GetAnalyzer",
        "access-analyzer:GetArchiveRule",
        "access-analyzer:ListAnalyzers",
```

```
        "access-analyzer:ListArchiveRules",
        "access-analyzer:ListTagsForResource",
        "account:GetAlternateContact",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:GetCertificateAuthorityCsr",
        "acm-pca:ListCertificateAuthorities",
        "acm-pca:ListTags",
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "acm:ListTagsForCertificate",
        "airflow:GetEnvironment",
        "airflow:ListEnvironments",
        "airflow:ListTagsForResource",
        "amplify:GetApp",
        "amplify:GetBranch",
        "amplify:ListApps",
        "amplify:ListBranches",
        "amplifyuibuilder:ExportThemes",
        "amplifyuibuilder:GetTheme",
        "amplifyuibuilder:ListThemes",
        "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:GetEventIntegration",
        "app-integrations:ListApplications",
        "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",
        "appmesh:DescribeGatewayRoute",
        "appmesh:DescribeMesh",
        "appmesh:DescribeRoute",
        "appmesh:DescribeVirtualGateway",
        "appmesh:DescribeVirtualNode",
        "appmesh:DescribeVirtualRouter",
        "appmesh:DescribeVirtualService",
        "appmesh:ListGatewayRoutes",
        "appmesh:ListMeshes",
        "appmesh:ListRoutes",
        "appmesh:ListTagsForResource",
        "appmesh:ListVirtualGateways",
        "appmesh:ListVirtualNodes",
        "appmesh:ListVirtualRouters",
        "appmesh:ListVirtualServices",
        "apprunner:DescribeService",
        "apprunner:DescribeVpcConnector",
        "apprunner:ListServices",
        "apprunner:ListTagsForResource",
        "apprunner:ListVpcConnectors",
        "appstream:DescribeAppBlockBuilders",
        "appstream:DescribeApplications",
        "appstream:DescribeDirectoryConfigs",
        "appstream:DescribeFleets",
        "appstream:DescribeStacks",
        "appstream:ListTagsForResource",
```

```
        "appsync:GetApiCache",
        "appsync:GetGraphqlApi",
        "appsync:ListGraphqlApis",
        "aps:DescribeAlertManagerDefinition",
        "aps:DescribeLoggingConfiguration",
        "APS:DescribeRuleGroupsNamespace",
        "APS:DescribeWorkspace",
        "aps:ListRuleGroupsNamespaces",
        "aps:ListTagsForResource",
        "APS:ListWorkspaces",
        "athena:GetDataCatalog",
        "athena:GetPreparedStatement",
        "athena:GetWorkGroup",
        "athena:ListDataCatalogs",
        "athena:ListPreparedStatements",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups",
        "auditmanager:GetAccountStatus",
        "auditmanager:GetAssessment",
        "auditmanager:ListAssessments",
        "autoscaling-plans:DescribeScalingPlanResources",
        "autoscaling-plans:DescribeScalingPlans",
        "autoscaling-plans:GetScalingPlanResourceForecastData",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeLaunchConfigurations",
        "autoscaling:DescribeLifecycleHooks",
        "autoscaling:DescribePolicies",
        "autoscaling:DescribeScheduledActions",
        "autoscaling:DescribeTags",
        "autoscaling:DescribeWarmPool",
        "b2bi:GetPartnership",
        "b2bi:GetProfile",
        "b2bi:ListPartnerships",
        "b2bi:ListProfiles",
        "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:GetAgent",
        "bedrock:GetAgentActionGroup",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:GetDataSource",
        "bedrock:GetFlowAlias",
        "bedrock:GetFlowVersion",
        "bedrock:GetGuardrail",
        "bedrock:GetInferenceProfile",
        "bedrock:GetKnowledgeBase",
        "bedrock:ListAgentActionGroups",
        "bedrock:ListAgentKnowledgeBases",
        "bedrock:ListAgents",
        "bedrock:ListDataSources",
        "bedrock:ListFlowAliases",
        "bedrock:ListFlowVersions",
        "bedrock:ListGuardrails",
        "bedrock:ListInferenceProfiles",
        "bedrock:ListKnowledgeBases",
        "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:GetAnomalyMonitors",
        "ce:GetAnomalySubscriptions",
        "cleanrooms-ml:GetTrainingDataset",
        "cleanrooms-ml:ListTrainingDatasets",
        "cleanrooms:GetConfiguredTable",
        "cleanrooms:GetConfiguredTableAnalysisRule",
        "cleanrooms:GetMembership",
        "cleanrooms:GetPrivacyBudgetTemplate",
        "cleanrooms:ListConfiguredTables",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListPrivacyBudgetTemplates",
        "cloud9:DescribeEnvironmentMemberships",
        "cloud9:DescribeEnvironments",
        "cloud9:ListEnvironments",
        "cloud9:ListTagsForResource",
        "cloudformation:BatchDescribeTypeConfigurations",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeType",
        "cloudformation:GetResource",
        "cloudformation:ListResources",
        "cloudformation:ListStackInstances",
        "cloudformation:ListStackResources",
        "cloudformation:ListStacks",
        "cloudformation:ListStackSets",
        "cloudformation:ListTypes",
        "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:GetEventDataStore",
        "cloudtrail:GetEventSelectors",
        "cloudtrail:GetInsightSelectors",
        "cloudtrail:GetTrailStatus",
        "cloudTrail:ListChannels",
        "cloudtrail:ListEventDataStores",
        "cloudtrail:ListTags",
        "cloudtrail:ListTrails",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:DescribeAnomalyDetectors",
        "cloudwatch:GetDashboard",
        "cloudwatch:GetMetricStream",
        "cloudwatch:ListDashboards",
        "cloudwatch:ListMetricStreams",
        "cloudwatch:ListTagsForResource",
        "codeartifact:DescribeRepository",
        "codeartifact:GetRepositoryPermissionsPolicy",
        "codeartifact:ListDomains",
        "codeartifact:ListPackages",
        "codeartifact:ListPackageVersions",
        "codeartifact:ListRepositories",
        "codeartifact:ListTagsForResource",
        "codebuild:BatchGetReportGroups",
        "codebuild:ListReportGroups",
        "codecommit:GetRepository",
        "codecommit:GetRepositoryTriggers",
        "codecommit:ListRepositories",
        "codecommit:ListTagsForResource",
        "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:ListPipelines",
        "cognito-identity:DescribeIdentityPool",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:GetPrincipalTagAttributeMap",
        "cognito-identity:ListIdentityPools",
        "cognito-identity:ListTagsForResource",
        "cognito-idp:DescribeIdentityProvider",
        "cognito-idp:DescribeResourceServer",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:DescribeUserPoolDomain",
        "cognito-idp:GetGroup",
        "cognito-idp:GetUserPoolMfaConfig",
        "cognito-idp:ListGroups",
        "cognito-idp:ListIdentityProviders",
        "cognito-idp:ListResourceServers",
        "cognito-idp:ListTagsForResource",
        "cognito-idp:ListUserPoolClients",
        "cognito-idp:ListUserPools",
        "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:DescribePrompt",
        "connect:DescribeQueue",
        "connect:DescribeQuickConnect",
        "connect:DescribeRoutingProfile",
        "connect:DescribeRule",
        "connect:DescribeSecurityProfile",
        "connect:DescribeUser",
        "connect:GetTaskTemplate",
        "connect:ListApprovedOrigins",
        "connect:ListEvaluationForms",
```

```
        "connect:ListInstanceAttributes",
        "connect:ListInstances",
        "connect:ListInstanceStorageConfigs",
        "connect:ListIntegrationAssociations",
        "connect:ListPhoneNumbers",
        "connect:ListPhoneNumbersV2",
        "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:ListUsers",
        "connect:SearchAvailablePhoneNumbers",
        "databrew:DescribeDataset",
        "databrew:DescribeJob",
        "databrew:DescribeProject",
        "databrew:DescribeRecipe",
        "databrew:DescribeRuleset",
        "databrew:DescribeSchedule",
        "databrew:ListDatasets",
        "databrew:ListJobs",
        "databrew:ListProjects",
        "databrew:ListRecipes",
        "databrew:ListRecipeVersions",
        "databrew:ListRulesets",
        "databrew:ListSchedules",
        "datasync:DescribeAgent",
        "datasync:DescribeLocationEfs",
        "datasync:DescribeLocationFsxLustre",
        "datasync:DescribeLocationFsxWindows",
        "datasync:DescribeLocationHdfs",
        "datasync:DescribeLocationNfs",
        "datasync:DescribeLocationObjectStorage",
        "datasync:DescribeLocationS3",
        "datasync:DescribeLocationSmb",
        "datasync:DescribeTask",
```

```
        "datasync:ListAgents",
        "datasync:ListLocations",
        "datasync:ListTagsForResource",
        "datasync:ListTasks",
        "datazone:GetDomain",
        "datazone:ListDomains",
        "dax:DescribeClusters",
        "dax:DescribeParameterGroups",
        "dax:DescribeParameters",
        "dax:DescribeSubnetGroups",
        "dax:ListTags",
        "detective:ListGraphs",
        "detective:ListTagsForResource",
        "devicefarm:GetInstanceProfile",
        "devicefarm:GetNetworkProfile",
        "devicefarm:GetProject",
        "devicefarm:GetTestGridProject",
        "devicefarm:ListInstanceProfiles",
        "devicefarm:ListNetworkProfiles",
        "devicefarm:ListProjects",
        "devicefarm:ListTagsForResource",
        "devicefarm:ListTestGridProjects",
        "devops-guru:GetResourceCollection",
        "devops-guru:ListNotificationChannels",
        "directconnect:DescribeConnections",
        "dms:DescribeCertificates",
        "dms:DescribeEndpoints",
        "dms:DescribeEventSubscriptions",
        "dms:DescribeReplicationConfigs",
        "dms:DescribeReplicationInstances",
        "dms:DescribeReplicationSubnetGroups",
        "dms:DescribeReplicationTaskAssessmentRuns",
        "dms:DescribeReplicationTasks",
        "dms:ListTagsForResource",
        "ds:DescribeDirectories",
        "ds:DescribeDomainControllers",
        "ds:DescribeEventTopics",
        "ds:ListLogSubscriptions",
        "ds:ListTagsForResource",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeGlobalTable",
        "dynamodb:DescribeGlobalTableSettings",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeTable",
```

```
        "dynamodb:DescribeTableReplicaAutoScaling",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:ListTables",
        "dynamodb:ListTagsOfResource",
        "ec2:Describe*",
        "ec2:DescribeClientVpnAuthorizationRules",
        "ec2:DescribeClientVpnEndpoints",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeFleets",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSpotFleetRequests",
        "ec2:DescribeTags",
        "ec2:DescribeTrafficMirrorFilters",
        "ec2:DescribeTrafficMirrorSessions",
        "ec2:DescribeTrafficMirrorTargets",
        "ec2:DescribeVolumeAttribute",
        "ec2:DescribeVolumes",
        "ec2:GetAllowedImagesSettings",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetInstanceTypesFromInstanceRequirements",
        "ec2:GetIpamPoolAllocations",
        "ec2:GetIpamPoolCidrs",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetNetworkInsightsAccessScopeAnalysisFindings",
        "ec2:GetNetworkInsightsAccessScopeContent",
        "ec2:GetSnapshotBlockPublicAccessState",
        "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:DescribeAddon",
        "eks:DescribeCluster",
        "eks:DescribeFargateProfile",
        "eks:DescribeIdentityProviderConfig",
        "eks:DescribeNodegroup",
        "eks:ListAddons",
        "eks:ListClusters",
        "eks:ListFargateProfiles",
        "eks:ListIdentityProviderConfigs",
        "eks:ListNodegroups",
        "eks:ListTagsForResource",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeCacheParameterGroups",
        "elasticache:DescribeCacheParameters",
        "elasticache:DescribeCacheSecurityGroups",
        "elasticache:DescribeCacheSubnetGroups",
        "elasticache:DescribeGlobalReplicationGroups",
        "elasticache:DescribeReplicationGroups",
        "elasticache:DescribeSnapshots",
        "elasticache:DescribeUserGroups",
        "elasticache:DescribeUsers",
        "elasticache:ListTagsForResource",
        "elasticbeanstalk:DescribeConfigurationSettings",
        "elasticbeanstalk:DescribeEnvironments",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeBackupPolicy",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeMountTargetSecurityGroups",
        "elasticfilesystem:DescribeTags",
        "elasticloadbalancing:DescribeListenerCertificates",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancerPolicies",
        "elasticloadbalancing:DescribeLoadBalancers",
```

```
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:DescribeSecurityConfiguration",
        "elasticmapreduce:DescribeStep",
        "elasticmapreduce:DescribeStudio",
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:GetManagedScalingPolicy",
        "elasticmapreduce:GetStudioSessionMapping",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListInstanceFleets",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListSecurityConfigurations",
        "elasticmapreduce:ListSteps",
        "elasticmapreduce:ListStudios",
        "elasticmapreduce:ListStudioSessionMappings",
        "emr-containers: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:GetSchemaMapping",
        "entityresolution:ListIdMappingWorkflows",
        "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:DescribeFleetAttributes",
        "gamelift:DescribeFleetCapacity",
        "gamelift:DescribeFleetLocationAttributes",
        "gamelift:DescribeFleetLocationCapacity",
        "gamelift:DescribeFleetPortSettings",
        "gamelift:DescribeGameServerGroup",
        "gamelift:DescribeGameSessionQueues",
        "gamelift:DescribeMatchmakingConfigurations",
        "gamelift:DescribeMatchmakingRuleSets",
        "gamelift:DescribeRuntimeConfiguration",
        "gamelift:DescribeScript",
        "gamelift:DescribeVpcPeeringAuthorizations",
        "gamelift:DescribeVpcPeeringConnections",
        "gamelift:ListAliases",
        "gamelift:ListBuilds",
        "gamelift:ListFleets",
        "gamelift:ListGameServerGroups",
        "gamelift:ListScripts",
        "gamelift:ListTagsForResource",
        "geo:DescribeGeofenceCollection",
        "geo:DescribeMap",
        "geo:DescribePlaceIndex",
        "geo:DescribeRouteCalculator",
        "geo:DescribeTracker",
        "geo:ListGeofenceCollections",
        "geo:ListMaps",
        "geo:ListPlaceIndexes",
        "geo:ListRouteCalculators",
        "geo:ListTrackerConsumers",
        "geo:ListTrackers",
        "globalaccelerator:DescribeAccelerator",
        "globalaccelerator:DescribeEndpointGroup",
        "globalaccelerator:DescribeListener",
```

```
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListEndpointGroups",
        "globalaccelerator:ListListeners",
        "globalaccelerator:ListTagsForResource",
        "glue:BatchGetDevEndpoints",
        "glue:BatchGetJobs",
        "glue:BatchGetWorkflows",
        "glue:GetClassifier",
        "glue:GetClassifiers",
        "glue:GetCrawler",
        "glue:GetCrawlers",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetDevEndpoint",
        "glue:GetDevEndpoints",
        "glue:GetJob",
        "glue:GetJobs",
        "glue:GetMLTransform",
        "glue:GetMLTransforms",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue: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:GetMasterAccount",
        "guardduty:GetMemberDetectors",
        "guardduty:GetMembers",
        "guardduty:GetThreatIntelSet",
        "guardduty:ListDetectors",
        "guardduty:ListFilters",
        "guardduty:ListFindings",
        "guardduty:ListIPSets",
        "guardduty:ListMembers",
        "guardduty:ListOrganizationAdminAccounts",
        "guardduty:ListPublishingDestinations",
        "guardduty:ListTagsForResource",
        "guardduty:ListThreatIntelSets",
        "healthlake:DescribeFHIRDatastore",
        "healthlake:ListFHIRDatastores",
        "healthlake:ListTagsForResource",
        "iam:GenerateCredentialReport",
        "iam:GetAccountAuthorizationDetails",
        "iam:GetAccountPasswordPolicy",
        "iam:GetAccountSummary",
        "iam:GetCredentialReport",
        "iam:GetGroup",
        "iam:GetGroupPolicy",
        "iam:GetInstanceProfile",
        "iam:GetOpenIDConnectProvider",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:GetSAMLProvider",
        "iam:GetServerCertificate",
        "iam:GetUser",
```

```
        "iam:GetUserPolicy",
        "iam:ListAccessKeys",
        "iam:ListAttachedGroupPolicies",
        "iam:ListAttachedRolePolicies",
        "iam:ListAttachedUserPolicies",
        "iam:ListEntitiesForPolicy",
        "iam:ListGroupPolicies",
        "iam:ListGroups",
        "iam:ListGroupsForUser",
        "iam:ListInstanceProfiles",
        "iam:ListInstanceProfilesForRole",
        "iam:ListInstanceProfileTags",
        "iam:ListMFADevices",
        "iam:ListMFADeviceTags",
        "iam:ListOpenIDConnectProviders",
        "iam:ListPolicyVersions",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListSAMLProviders",
        "iam:ListServerCertificates",
        "iam:ListUserPolicies",
        "iam:ListUsers",
        "iam:ListVirtualMFADevices",
        "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: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",
        "iot:DescribeAccountAuditConfiguration",
        "iot:DescribeAuthorizer",
        "iot:DescribeBillingGroup",
        "iot:DescribeCACertificate",
        "iot:DescribeCertificate",
        "iot:DescribeCustomMetric",
        "iot:DescribeDimension",
        "iot:DescribeDomainConfiguration",
        "iot:DescribeFleetMetric",
        "iot:DescribeJobTemplate",
        "iot:DescribeMitigationAction",
        "iot:DescribeProvisioningTemplate",
        "iot:DescribeRoleAlias",
        "iot:DescribeScheduledAudit",
        "iot:DescribeSecurityProfile",
        "iot:DescribeThingGroup",
        "iot:DescribeThingType",
        "iot:GetPolicy",
        "iot:GetTopicRule",
        "iot:GetTopicRuleDestination",
        "iot:ListAuthorizers",
        "iot:ListBillingGroups",
        "iot:ListCACertificates",
        "iot:ListCertificates",
        "iot:ListCustomMetrics",
        "iot:ListDimensions",
        "iot:ListDomainConfigurations",
        "iot:ListFleetMetrics",
        "iot:ListJobTemplates",
        "iot:ListMitigationActions",
        "iot:ListPolicies",
        "iot:ListProvisioningTemplates",
        "iot:ListRoleAliases",
        "iot:ListScheduledAudits",
        "iot:ListSecurityProfiles",
        "iot:ListSecurityProfilesForTarget",
        "iot:ListTagsForResource",
        "iot:ListTargetsForSecurityProfile",
        "iot: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:ListAssetModels",
        "iotsitewise:ListAssets",
        "iotsitewise:ListDashboards",
        "iotsitewise:ListGateways",
        "iotsitewise:ListPortals",
        "iotsitewise:ListProjectAssets",
        "iotsitewise:ListProjects",
        "iotsitewise:ListTagsForResource",
        "iottwinmaker:GetComponentType",
        "iottwinmaker:GetEntity",
        "iottwinmaker:GetScene",
        "iottwinmaker:GetSyncJob",
        "iottwinmaker:GetWorkspace",
        "iottwinmaker:ListComponentTypes",
        "iottwinmaker:ListEntities",
        "iottwinmaker:ListScenes",
        "iottwinmaker:ListSyncJobs",
        "iottwinmaker:ListTagsForResource",
        "iottwinmaker:ListWorkspaces",
        "iotwireless:GetDestination",
        "iotwireless:GetDeviceProfile",
        "iotwireless:GetFuotaTask",
        "iotwireless:GetMulticastGroup",
        "iotwireless:GetServiceProfile",
        "iotwireless:GetWirelessDevice",
        "iotwireless:GetWirelessGateway",
        "iotwireless:GetWirelessGatewayTaskDefinition",
        "iotwireless:ListDestinations",
        "iotwireless:ListDeviceProfiles",
        "iotwireless:ListFuotaTasks",
        "iotwireless:ListMulticastGroups",
        "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: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:ListConnectors",
        "kendra:DescribeIndex",
        "kendra:ListIndices",
        "kendra:ListTagsForResource",
        "kinesis:DescribeStreamConsumer",
        "kinesis:DescribeStreamSummary",
        "kinesis:ListStreamConsumers",
        "kinesis:ListStreams",
        "kinesis:ListTagsForStream",
        "kinesisanalytics:DescribeApplication",
        "kinesisanalytics:ListApplications",
        "kinesisanalytics:ListTagsForResource",
        "kinesisvideo:DescribeSignalingChannel",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:ListSignalingChannels",
```

```
        "kinesisvideo:ListStreams",
        "kinesisvideo:ListTagsForResource",
        "kinesisvideo:ListTagsForStream",
        "kms:DescribeKey",
        "kms:GetKeyPolicy",
        "kms:GetKeyRotationStatus",
        "kms:ListAliases",
        "kms:ListKeys",
        "kms:ListResourceTags",
        "lakeformation:DescribeResource",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:ListPermissions",
        "lakeformation:ListResources",
        "lambda:GetAlias",
        "lambda:GetCodeSigningConfig",
        "lambda:GetEventSourceMapping",
        "lambda:GetFunction",
        "lambda:GetFunctionCodeSigningConfig",
        "lambda:GetLayerVersion",
        "lambda:GetPolicy",
        "lambda:ListAliases",
        "lambda:ListCodeSigningConfigs",
        "lambda:ListEventSourceMappings",
        "lambda:ListFunctions",
        "lambda:ListLayers",
        "lambda:ListLayerVersions",
        "lambda:ListTags",
        "lambda:ListVersionsByFunction",
        "lex:DescribeBot",
        "lex:DescribeBotAlias",
        "lex:DescribeBotVersion",
        "lex:DescribeResourcePolicy",
        "lex:ListBotAliases",
        "lex:ListBotLocales",
        "lex:ListBots",
        "lex:ListBotVersions",
        "lex:ListTagsForResource",
        "license-manager:GetGrant",
        "license-manager:GetLicense",
        "license-manager:ListDistributedGrants",
        "license-manager:ListLicenses",
        "license-manager:ListReceivedGrants",
        "lightsail:GetAlarms",
        "lightsail:GetBuckets",
```

```
        "lightsail:GetCertificates",
        "lightsail:GetContainerServices",
        "lightsail:GetDisk",
        "lightsail:GetDisks",
        "lightsail:GetDistributions",
        "lightsail:GetInstance",
        "lightsail:GetInstances",
        "lightsail:GetKeyPair",
        "lightsail:GetLoadBalancer",
        "lightsail:GetLoadBalancers",
        "lightsail:GetLoadBalancerTlsCertificates",
        "lightsail:GetRelationalDatabase",
        "lightsail:GetRelationalDatabaseParameters",
        "lightsail:GetRelationalDatabases",
        "lightsail:GetStaticIp",
        "lightsail:GetStaticIps",
        "logs:DescribeAccountPolicies",
        "logs:DescribeDestinations",
        "logs:DescribeLogGroups",
        "logs:DescribeMetricFilters",
        "logs:DescribeResourcePolicies",
        "logs:GetDataProtectionPolicy",
        "logs:GetLogAnomalyDetector",
        "logs:GetLogDelivery",
        "logs:ListLogAnomalyDetectors",
        "logs:ListLogDeliveries",
        "logs:ListTagsLogGroup",
        "lookoutequipment:DescribeInferenceScheduler",
        "lookoutequipment:ListTagsForResource",
        "lookoutmetrics:DescribeAlert",
        "lookoutmetrics:DescribeAnomalyDetector",
        "lookoutmetrics:ListAlerts",
        "lookoutmetrics:ListAnomalyDetectors",
        "lookoutmetrics:ListMetricSets",
        "lookoutmetrics:ListTagsForResource",
        "lookoutvision:DescribeProject",
        "lookoutvision:ListProjects",
        "m2:GetEnvironment",
        "m2:ListEnvironments",
        "m2:ListTagsForResource",
        "macie2:DescribeOrganizationConfiguration",
        "macie2:GetAutomatedDiscoveryConfiguration",
        "macie2:GetClassificationExportConfiguration",
        "macie2:GetCustomDataIdentifier",
```

```
        "macie2:GetFindingsPublicationConfiguration",
        "macie2:GetMacieSession",
        "macie2: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",
        "mediapackage-vod:DescribePackagingConfiguration",
        "mediapackage-vod:DescribePackagingGroup",
        "mediapackage-vod:ListPackagingConfigurations",
        "mediapackage-vod:ListPackagingGroups",
        "mediapackage-vod:ListTagsForResource",
        "mediapackagev2:GetChannel",
        "mediapackagev2:ListChannels",
        "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",
        "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:GetDirectoryRegistration",
        "pca-connector-ad:ListDirectoryRegistrations",
```

```
        "pca-connector-ad:ListTagsForResource",
        "personalize:DescribeDataset",
        "personalize:DescribeDatasetGroup",
        "personalize:DescribeSchema",
        "personalize:DescribeSolution",
        "personalize:ListDatasetGroups",
        "personalize:ListDatasetImportJobs",
        "personalize:ListDatasets",
        "personalize:ListSchemas",
        "personalize:ListSolutions",
        "personalize:ListTagsForResource",
        "profile:GetDomain",
        "profile:GetIntegration",
        "profile:GetProfileObjectType",
        "profile:ListDomains",
        "profile:ListIntegrations",
        "profile:ListProfileObjectTypes",
        "profile:ListTagsForResource",
        "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:DescribeTemplate",
        "quicksight:DescribeTemplatePermissions",
        "quicksight:DescribeTheme",
        "quicksight:DescribeThemePermissions",
        "quicksight:ListAnalyses",
        "quicksight:ListDashboards",
        "quicksight:ListDataSets",
        "quicksight:ListDataSources",
        "quicksight:ListTagsForResource",
        "quicksight:ListTemplates",
        "quicksight:ListThemes",
        "ram:GetPermission",
        "ram:GetResourceShareAssociations",
```

```
        "ram:GetResourceShares",
        "ram:ListPermissionAssociations",
        "ram:ListPermissions",
        "ram:ListPermissionVersions",
        "ram:ListResources",
        "ram:ListResourceSharePermissions",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBProxies",
        "rds:DescribeDBProxyEndpoints",
        "rds:DescribeDBProxyTargetGroups",
        "rds:DescribeDBProxyTargets",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBShardGroups",
        "rds:DescribeDBSnapshotAttributes",
        "rds:DescribeDBSnapshots",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultClusterParameters",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeGlobalClusters",
        "rds:DescribeIntegrations",
        "rds:DescribeOptionGroups",
        "rds:ListTagsForResource",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:ListWorkgroups",
        "redshift:DescribeClusterParameterGroups",
        "redshift:DescribeClusterParameters",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSecurityGroups",
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeClusterSubnetGroups",
        "redshift:DescribeEndpointAccess",
        "redshift:DescribeEndpointAuthorization",
        "redshift:DescribeEventSubscriptions",
```

```
        "redshift:DescribeIntegrations",
        "redshift:DescribeLoggingStatus",
        "redshift:DescribeScheduledActions",
        "redshift:DescribeTags",
        "refactor-spaces:GetEnvironment",
        "refactor-spaces:GetService",
        "refactor-spaces:ListApplications",
        "refactor-spaces:ListEnvironments",
        "refactor-spaces:ListServices",
        "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",
        "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:GetAccessGrantsInstance",
        "s3:GetAccessGrantsLocation",
        "s3:GetAccessPoint",
        "s3:GetAccessPointForObjectLambda",
        "s3:GetAccessPointPolicy",
        "s3:GetAccessPointPolicyForObjectLambda",
        "s3:GetAccessPointPolicyStatus",
        "s3:GetAccessPointPolicyStatusForObjectLambda",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketCORS",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketNotification",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketRequestPayment",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "s3:GetBucketWebsite",
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetMultiRegionAccessPoint",
        "s3:GetMultiRegionAccessPointPolicy",
        "s3:GetMultiRegionAccessPointPolicyStatus",
        "s3:GetReplicationConfiguration",
```

```
        "s3:GetStorageLensConfiguration",
        "s3:GetStorageLensConfigurationTagging",
        "s3:GetStorageLensGroup",
        "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:ListTableBuckets",
        "sagemaker:DescribeAppImageConfig",
        "sagemaker:DescribeCluster",
        "sagemaker:DescribeCodeRepository",
        "sagemaker:DescribeDataQualityJobDefinition",
        "sagemaker:DescribeDeviceFleet",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeFeatureGroup",
        "sagemaker:DescribeImage",
        "sagemaker:DescribeImageVersion",
        "sagemaker:DescribeInferenceExperiment",
        "sagemaker:DescribeMlflowTrackingServer",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeModelBiasJobDefinition",
        "sagemaker:DescribeModelExplainabilityJobDefinition",
        "sagemaker:DescribeModelQualityJobDefinition",
        "sagemaker:DescribeMonitoringSchedule",
        "sagemaker:DescribeNotebookInstance",
        "sagemaker:DescribeNotebookInstanceLifecycleConfig",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribeProject",
        "sagemaker:DescribeStudioLifecycleConfig",
```

```
        "sagemaker:DescribeWorkteam",
        "sagemaker:ListAppImageConfigs",
        "sagemaker:ListClusters",
        "sagemaker:ListCodeRepositories",
        "sagemaker:ListDataQualityJobDefinitions",
        "sagemaker:ListDeviceFleets",
        "sagemaker:ListDomains",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListEndpoints",
        "sagemaker:ListFeatureGroups",
        "sagemaker:ListImages",
        "sagemaker:ListImageVersions",
        "sagemaker:ListInferenceExperiments",
        "sagemaker:ListMlflowTrackingServers",
        "sagemaker:ListModelBiasJobDefinitions",
        "sagemaker:ListModelExplainabilityJobDefinitions",
        "sagemaker:ListModelQualityJobDefinitions",
        "sagemaker:ListModels",
        "sagemaker:ListMonitoringSchedules",
        "sagemaker:ListNotebookInstanceLifecycleConfigs",
        "sagemaker:ListNotebookInstances",
        "sagemaker:ListPipelines",
        "sagemaker:ListProjects",
        "sagemaker:ListStudioLifecycleConfigs",
        "sagemaker:ListTags",
        "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:ListSecrets",
        "secretsmanager:ListSecretVersionIds",
        "securityhub:DescribeHub",
        "securityhub:DescribeStandardsControls",
```

```
        "securityhub:GetEnabledStandards",
        "serviceCatalog:DescribePortfolioShares",
        "servicediscovery:GetInstance",
        "servicediscovery:GetNamespace",
        "servicediscovery:GetService",
        "servicediscovery:ListInstances",
        "servicediscovery:ListNamespaces",
        "servicediscovery:ListServices",
        "servicediscovery:ListTagsForResource",
        "ses:DescribeReceiptRule",
        "ses:DescribeReceiptRuleSet",
        "ses:GetConfigurationSet",
        "ses:GetConfigurationSetEventDestinations",
        "ses:GetContactList",
        "ses:GetDedicatedIpPool",
        "ses:GetDedicatedIps",
        "ses:GetEmailTemplate",
        "ses:GetTemplate",
        "ses:ListConfigurationSets",
        "ses:ListContactLists",
        "ses:ListDedicatedIpPools",
        "ses:ListEmailTemplates",
        "ses:ListReceiptFilters",
        "ses:ListReceiptRuleSets",
        "ses:ListTemplates",
        "shield:DescribeDRTAccess",
        "shield:DescribeProtection",
        "shield:DescribeSubscription",
        "signer:GetSigningProfile",
        "signer:ListProfilePermissions",
        "signer:ListSigningProfiles",
        "sns:GetDataProtectionPolicy",
        "sns:GetSMSSandboxAccountStatus",
        "sns:GetSubscriptionAttributes",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTagsForResource",
        "sns:ListTopics",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues",
        "sqs:ListQueueTags",
        "ssm-contacts:GetContact",
        "ssm-contacts:GetContactChannel",
```

```
        "ssm-contacts:ListContactChannels",
        "ssm-contacts:ListContacts",
        "ssm-incidents:GetResponsePlan",
        "ssm-incidents:ListResponsePlans",
        "ssm-incidents:ListTagsForResource",
        "ssm-quicksetup:GetConfigurationManager",
        "ssm-quicksetup:ListConfigurationManagers",
        "ssm-sap:ListTagsForResource",
        "ssm:DescribeAutomationExecutions",
        "ssm:DescribeDocument",
        "ssm:DescribeDocumentPermission",
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeParameters",
        "ssm:GetAutomationExecution",
        "ssm:GetDocument",
        "ssm:GetServiceSetting",
        "ssm:ListDocuments",
        "ssm:ListTagsForResource",
        "sso:DescribeInstanceAccessControlAttributeConfiguration",
        "sso:DescribePermissionSet",
        "sso:GetInlinePolicyForPermissionSet",
        "sso:ListManagedPoliciesInPermissionSet",
        "sso:ListPermissionSets",
        "sso:ListTagsForResource",
        "states:DescribeActivity",
        "states:DescribeStateMachine",
        "states:ListActivities",
        "states:ListStateMachines",
        "states:ListTagsForResource",
        "storagegateway:ListGateways",
        "storagegateway:ListTagsForResource",
        "storagegateway:ListVolumes",
        "sts:GetCallerIdentity",
        "support:DescribeCases",
        "synthetics:DescribeCanaries",
        "synthetics:DescribeCanariesLastRun",
        "synthetics:DescribeRuntimeVersions",
        "synthetics:GetCanary",
        "synthetics:GetCanaryRuns",
        "synthetics:GetGroup",
        "synthetics:ListAssociatedGroups",
        "synthetics:ListGroupResources",
        "synthetics:ListGroups",
        "synthetics:ListTagsForResource",
```

```
        "tag:GetResources",
        "timestream:DescribeDatabase",
        "timestream:DescribeEndpoints",
        "timestream:DescribeTable",
        "timestream:ListDatabases",
        "timestream:ListTables",
        "timestream:ListTagsForResource",
        "transfer:DescribeAgreement",
        "transfer:DescribeCertificate",
        "transfer:DescribeConnector",
        "transfer:DescribeProfile",
        "transfer:DescribeServer",
        "transfer:DescribeUser",
        "transfer:DescribeWorkflow",
        "transfer:ListAgreements",
        "transfer:ListCertificates",
        "transfer:ListConnectors",
        "transfer:ListProfiles",
        "transfer:ListServers",
        "transfer:ListTagsForResource",
        "transfer:ListUsers",
        "transfer:ListWorkflows",
        "voiceid:DescribeDomain",
        "voiceid:ListTagsForResource",
        "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:ListRuleGroups",
        "wafv2:ListTagsForResource",
```

```
        "workspaces:DescribeConnectionAliases",
        "workspaces:DescribeTags",
        "workspaces:DescribeWorkspaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSConfigSLRLogStatementID",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/config/*"
    },
    {
      "Sid" : "AWSConfigSLRLogEventStatementID",
      "Effect" : "Allow",
      "Action" : "logs:PutLogEvents",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/config/*:log-stream:config-rule-
evaluation/*"
    },
    {
      "Sid" : "AWSConfigSLRApiGatewayStatementID",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/apis/*/integrations",
        "arn:aws:apigateway:*::/apis/*/integrations/*",
        "arn:aws:apigateway:*::/domainnames",
        "arn:aws:apigateway:*::/domainnames/*",
        "arn:aws:apigateway:*::/clientcertificates",
        "arn:aws:apigateway:*::/clientcertificates/*",
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/resources",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integration",
```

```
        "arn:aws:apigateway:*::/restapis/*/resources/*",
        "arn:aws:apigateway:*::/apis/*/routes/*",
        "arn:aws:apigateway:*::/apis/*/routes",
        "arn:aws:apigateway:*::/v2/apis/*/routes",
        "arn:aws:apigateway:*::/v2/apis/*/routes/*",
        "arn:aws:apigateway:*::/v2/apis",
        "arn:aws:apigateway:*::/v2/apis/*",
        "arn:aws:apigateway:*::/v2/apis/*/integrations",
        "arn:aws:apigateway:*::/v2/apis/*/integrations/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSConfigUserAccess

Deskripsi: Menyediakan akses untuk menggunakan AWS Config, termasuk mencari berdasarkan tag pada sumber daya, dan membaca semua tag. Ini tidak memberikan izin untuk mengonfigurasi AWS Config, yang memerlukan hak administratif.

`AWSConfigUserAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSConfigUserAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 Februari 2015, 19:38 UTC
- Waktu yang telah diedit: 18 Maret 2019, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSConfigUserAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "config:Get*",
        "config:Describe*",
        "config:Deliver*",
        "config:List*",
        "config:Select*",
        "tag:GetResources",
        "tag:GetTagKeys",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:LookupEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSConnector

Deskripsi: Mengaktifkan read/write akses luas ke SEMUA EC2 objek, read/write akses ke bucket S3 dimulai dengan 'import-to-ec2-', dan kemampuan untuk membuat daftar semua bucket S3, untuk AWS Konektor untuk mengimpor atas nama Anda. VMs

`AWSConnector`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSConnector` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 11 Februari 2015, 17:14 UTC
- Waktu telah diedit: 28 September 2015, 19:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSConnector`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteObject",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:AbortMultipartUpload",
        "s3:ListBucketMultipartUploads",
        "s3:ListMultipartUploadParts"
      ],
      "Resource" : "arn:aws:s3:::import-to-ec2-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CancelConversionTask",
        "ec2:CancelExportTask",
        "ec2:CreateImage",
        "ec2:CreateInstanceExportTask",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:DeleteTags",
        "ec2:DeleteVolume",
        "ec2:DescribeConversionTasks",
        "ec2:DescribeExportTasks",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances",
        "ec2:DescribeRegions",
        "ec2:DescribeTags",
        "ec2:DetachVolume",
        "ec2:ImportInstance",
        "ec2:ImportVolume",
        "ec2:ModifyInstanceAttribute",
```

```
        "ec2:RunInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:ImportImage",
        "ec2:DescribeImportImageTasks",
        "ec2:DeregisterImage",
        "ec2:DescribeSnapshots",
        "ec2:DeleteSnapshot",
        "ec2:CancelImportTask",
        "ec2:ImportSnapshot",
        "ec2:DescribeImportSnapshotTasks"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "SNS:Publish"
      ],
      "Resource" : "arn:aws:sns:*:*:metrics-sns-topic-for-*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSControlTowerAccountServiceRolePolicy

Deskripsi: Memungkinkan AWS Control Tower untuk memanggil AWS layanan yang menyediakan konfigurasi akun otomatis dan tata kelola terpusat atas nama Anda.

`AWSControlTowerAccountServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 05 Juni 2023, 22:04 UTC
- Waktu yang telah diedit: 03 Juni 2025, 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSControlTowerAccountServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowPutRuleOnSpecificSourcesAndDetailTypes",
      "Effect" : "Allow",
      "Action" : "events:PutRule",
      "Resource" : "arn:aws:events:*:*:rule/*ControlTower*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "events:source" : "aws.securityhub"
        },
        "Null" : {
          "events:detail-type" : "false"
        },
        "StringEquals" : {
```

```
          "events:ManagedBy" : "controltower.amazonaws.com",
          "events:detail-type" : "Security Hub Findings - Imported"
        }
      }
    },
    {
      "Sid" : "AllowOtherOperationsOnRulesManagedByControlTower",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:EnableRule",
        "events:DisableRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*ControlTower*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "controltower.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowDescribeOperationsOnRulesManagedByControlTower",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*ControlTower*"
    },
    {
      "Sid" : "AllowControlTowerToPublishSecurityNotifications",
      "Effect" : "Allow",
      "Action" : "sns:publish",
      "Resource" : "arn:aws:sns:*:*:aws-controltower-AggregateSecurityNotifications",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    },
    {
      "Sid" : "AllowActionsForSecurityHubIntegration",
```

```
      "Effect" : "Allow",
      "Action" : [
        "securityhub:DescribeStandardsControls",
        "securityhub:GetEnabledStandards"
      ],
      "Resource" : "arn:aws:securityhub:*:*:hub/default"
    },
    {
      "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" : "*"
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSControlTowerServiceRolePolicy

Deskripsi: Menyediakan akses ke AWS Sumber Daya yang dikelola atau digunakan oleh AWS Control Tower

`AWSControlTowerServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSControlTowerServiceRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 03 Mei 2019, 18:19 UTC
- Waktu telah diedit: 13 Januari 2025, 18:22 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSControlTowerServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v11 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:CreateStackInstances",
        "cloudformation:CreateStackSet",
        "cloudformation:DeleteStack",
        "cloudformation:DeleteStackInstances",
        "cloudformation:DeleteStackSet",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:ListStackInstances",
        "cloudformation:UpdateStack",
        "cloudformation:UpdateStackInstances",
        "cloudformation:UpdateStackSet"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:type/resource/AWS-IAM-Role"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:CreateStackInstances",
        "cloudformation:CreateStackSet",
        "cloudformation:DeleteStack",
        "cloudformation:DeleteStackInstances",
        "cloudformation:DeleteStackSet",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:GetTemplate",
        "cloudformation:ListStackInstances",
        "cloudformation:UpdateStack",
```

```
        "cloudformation:UpdateStackInstances",
        "cloudformation:UpdateStackSet"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/AWSControlTower*/*",
        "arn:aws:cloudformation:*:*:stack/StackSet-AWSControlTower*/*",
        "arn:aws:cloudformation:*:*:stackset/AWSControlTower*:*",
        "arn:aws:cloudformation:*:*:stackset-target/AWSControlTower*/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateTrail",
        "cloudtrail:DeleteTrail",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:StartLogging",
        "cloudtrail:StopLogging",
        "cloudtrail:UpdateTrail",
        "cloudtrail:PutEventSelectors",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:aws-controltower/CloudTrailLogs:*",
        "arn:aws:cloudtrail:*:*:trail/aws-controltower*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-controltower*/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : [
```

```
        "arn:aws:iam::*:role/AWSControlTowerExecution",
        "arn:aws:iam::*:role/AWSControlTowerBlueprintAccess"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:DescribeTrails",
        "ec2:DescribeAvailabilityZones",
        "iam:ListRoles",
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups",
        "organizations:CreateAccount",
        "organizations:DescribeAccount",
        "organizations:DescribeCreateAccountStatus",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribePolicy",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListChildren",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListPoliciesForTarget",
        "organizations:ListTargetsForPolicy",
        "organizations:ListRoots",
        "organizations:MoveAccount",
        "servicecatalog:AssociatePrincipalWithPortfolio"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetUser",
        "iam:ListAttachedRolePolicies",
        "iam:GetRolePolicy"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AWSControlTowerStackSetRole",
        "arn:aws:iam::*:role/service-role/AWSControlTowerCloudTrailRole",
        "arn:aws:iam::*:role/service-role/
AWSControlTowerConfigAggregatorRoleForOrganizations"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DeleteConfigurationAggregator",
        "config:PutConfigurationAggregator",
        "config:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/aws-control-tower" : "managed-by-control-tower"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:DisableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "organizations:ServicePrincipal" : [
            "config.amazonaws.com",
            "cloudtrail.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "cloudtrail.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "account:EnableRegion",
        "account:ListRegions",
        "account:GetRegionOptStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForCloudFormationHooksIntegration",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:SetTypeConfiguration",
        "cloudformation:DeactivateType",
        "cloudformation:ActivateType"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:type/hook/AWS-ControlTower*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCostAndUsageReportAutomationPolicy

Deskripsi: Memberikan izin untuk mendeskripsikan organisasi akun, membuat bucket S3 untuk program MAP dan menerapkan tag padanya, membuat Laporan Biaya dan Penggunaan, dan menjelaskan definisi Laporan Biaya dan Penggunaan.

`AWSCostAndUsageReportAutomationPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCostAndUsageReportAutomationPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 01 November 2021 21:27 UTC
- Waktu yang telah diedit: 01 November 2021, 21:27 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCostAndUsageReportAutomationPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
        "s3:GetBucketTagging",
        "s3:PutBucketTagging",
        "s3:GetBucketPolicy",
        "s3:PutBucketPolicy",
        "s3:ListBucket",
        "s3:CreateBucket"
      ],
      "Resource" : "arn:aws:s3:::aws-map-cur-bucket-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cur:PutReportDefinition",
        "cur:DeleteReportDefinition",
        "cur:DescribeReportDefinitions"
      ],
      "Resource" : "arn:aws:cur:*:*:definition/map-migrated-report"
    },
    {
      "Effect" : "Allow",
      "Action" : "cur:DescribeReportDefinitions",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSDataExchangeDataGrantOwnerFullAccess

Deskripsi: Memberi pemilik Data Grant akses ke tindakan AWS Data Exchange menggunakan AWS Management Console dan SDK.

`AWSDataExchangeDataGrantOwnerFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDataExchangeDataGrantOwnerFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 24 Oktober 2024, 14:43 UTC
- Waktu yang telah diedit: 24 Oktober 2024, 14:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeDataGrantOwnerFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSDataExchangeDataGrantReceiverFullAccess

Deskripsi: Memberikan akses penerima Data Grant ke tindakan AWS Data Exchange menggunakan AWS Management Console dan SDK.

`AWSDataExchangeDataGrantReceiverFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDataExchangeDataGrantReceiverFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 24 Oktober 2024, 14:45 UTC
- Waktu telah diedit: 24 Oktober 2024, 14:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeDataGrantReceiverFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSDataExchangeFullAccess

Deskripsi: Memberikan akses penuh ke AWS Data Exchange dan AWS Marketplace tindakan menggunakan AWS Management Console dan SDK. Ini juga menyediakan akses terpilih ke layanan terkait yang diperlukan untuk memanfaatkan sepenuhnya AWS Data Exchange.

`AWSDataExchangeFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDataExchangeFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 13 November 2019, 19:27 UTC

- Waktu yang telah diedit: 24 Juni 2024, 19:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeFullAccess`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSDataExchangeProviderFullAccess

Deskripsi: Memberikan akses penyedia data ke AWS Data Exchange dan AWS Marketplace tindakan menggunakan SDK AWS Management Console dan penyedia data. Ini juga menyediakan akses terpilih ke layanan terkait yang diperlukan untuk memanfaatkan sepenuhnya AWS Data Exchange.

`AWSDataExchangeProviderFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDataExchangeProviderFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 13 November 2019, 19:27 UTC
- Waktu telah diedit: Agustus 15, 2024, 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeProviderFullAccess`

Versi kebijakan

Versi kebijakan: v12 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSDataExchangeReadOnly

Deskripsi: Memberikan akses hanya-baca ke AWS Data Exchange dan AWS Marketplace tindakan menggunakan SDK dan. AWS Management Console

`AWSDataExchangeReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDataExchangeReadOnly` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 13 November 2019, 19:27 UTC
- Waktu telah diedit: 24 Oktober 2024, 14:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeReadOnly`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSDataExchangeServiceRolePolicyForLicenseManagement

Deskripsi: Memungkinkan AWS Data Exchange mengakses Layanan AWS dan Sumber Daya yang digunakan atau dikelola oleh AWS Data Exchange untuk manajemen lisensi.

`AWSDataExchangeServiceRolePolicyForLicenseManagement`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 10 Oktober 2024, 14:54 UTC
- Waktu yang telah diedit: 10 Oktober 2024, 14:54 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDataExchangeServiceRolePolicyForLicenseManagement`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSDataExchangeServiceRolePolicyForOrganizationDiscovery

Deskripsi: Memungkinkan AWS Data Exchange membaca data tentang AWS Organisasi Anda untuk menentukan kelayakan untuk AWS Data Exchange memberikan distribusi lisensi.

`AWSDataExchangeServiceRolePolicyForOrganizationDiscovery`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 10 Oktober 2024, 14:33 UTC
- Waktu yang telah diedit: 10 Oktober 2024, 14:33 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDataExchangeServiceRolePolicyForOrganizationDiscovery`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowAWSOrganizationsActions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "organizations:ListAccounts"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```


Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSDataExchangeSubscriberFullAccess

Deskripsi: Memberikan akses pelanggan data ke AWS Data Exchange dan AWS Marketplace tindakan menggunakan AWS Management Console dan SDK. Ini juga menyediakan akses terpilih ke layanan terkait yang diperlukan untuk memanfaatkan sepenuhnya AWS Data Exchange.

`AWSDataExchangeSubscriberFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDataExchangeSubscriberFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 13 November 2019, 19:27 UTC
- Waktu yang telah diedit: 21 Mei 2024, 17:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeSubscriberFullAccess`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSDataLifecycleManagerServiceRole

Deskripsi: Memberikan izin yang sesuai kepada Pengelola Siklus Hidup AWS Data untuk mengambil tindakan pada sumber daya AWS

`AWSDataLifecycleManagerServiceRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDataLifecycleManagerServiceRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 06 Juli 2018, 19:34 UTC
- Waktu yang telah diedit: 16 Desember 2024, 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDataLifecycleManagerServiceRole`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot",
        "ec2:CreateSnapshots",
        "ec2:DeleteSnapshot",
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots",
        "ec2:EnableFastSnapshotRestores",
        "ec2:DescribeFastSnapshotRestores",
        "ec2:DisableFastSnapshotRestores",
```

```
        "ec2:CopySnapshot",
        "ec2:ModifySnapshotAttribute",
        "ec2:DescribeSnapshotAttribute",
        "ec2:DescribeSnapshotTierStatus",
        "ec2:ModifySnapshotTier",
        "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.*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSDataLifecycleManagerServiceRoleForAMIManagement

Deskripsi: Memberikan izin yang sesuai kepada Manajer Siklus Hidup AWS Data untuk mengambil tindakan pada sumber daya AWS untuk Manajemen AMI

`AWSDataLifecycleManagerServiceRoleForAMIManagement`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDataLifecycleManagerServiceRoleForAMIManagement` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 21 Oktober 2020 19:39 UTC
- Waktu yang telah diedit: 19 Agustus 2021, 17:03 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDataLifecycleManagerServiceRoleForAMIManagement`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*",
```

```
        "arn:aws:ec2:*::image/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeImageAttribute",
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:DeleteSnapshot",
      "Resource" : "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ResetImageAttribute",
        "ec2:DeregisterImage",
        "ec2:CreateImage",
        "ec2:CopyImage",
        "ec2:ModifyImageAttribute"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:EnableImageDeprecation",
        "ec2:DisableImageDeprecation"
      ],
      "Resource" : "arn:aws:ec2:*::image/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSDataLifecycleManagerSSMFullAccess

Deskripsi: Memberikan izin Amazon Data Lifecycle Manager untuk melakukan tindakan Systems Manager yang diperlukan untuk menjalankan skrip pra dan pasca di semua instans Amazon. EC2

`AWSDataLifecycleManagerSSMFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDataLifecycleManagerSSMFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 31 Oktober 2023, 20:29 UTC
- Waktu telah diedit: 16 November 2023, 22:31 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDataLifecycleManagerSSMFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSSMReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetCommandInvocation",
        "ssm:ListCommands",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowTaggedSSMDocumentsOnly",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:DescribeDocument",
        "ssm:GetDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/DLMScriptsAccess" : "true"
        }
      }
    },
    {
      "Sid" : "AllowSpecificAWSOwnedSSMDocuments",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:DescribeDocument",
        "ssm:GetDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSEC2-CreateVssSnapshot",
        "arn:aws:ssm:*:*:document/AWSSystemsManagerSAP-CreateDLMSnapshotForSAPHANA"
```

```
      ]
    },
    {
      "Sid" : "AllowAllEC2Instances",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSDataPipeline_FullAccess

Deskripsi: Menyediakan akses penuh ke Data Pipeline, akses daftar untuk peran S3, DynamoDB, Redshift, RDS, SNS, dan IAM, dan akses PassRole untuk Peran default.

`AWSDataPipeline_FullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDataPipeline_FullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 19 Januari 2017, 23:14 UTC
- Waktu telah diedit: 17 Agustus 2017, 18:48 UTC

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

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "s3:List*",
        "dynamodb:DescribeTable",
        "rds:DescribeDBInstances",
        "rds:DescribeDBSecurityGroups",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSecurityGroups",
        "sns:ListTopics",
        "sns:Subscribe",
        "iam:ListRoles",
        "iam:GetRolePolicy",
        "iam:GetInstanceProfile",
        "iam:ListInstanceProfiles",
        "datapipeline:*"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Action" : "iam:PassRole",
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/DataPipelineDefaultResourceRole",
        "arn:aws:iam::*:role/DataPipelineDefaultRole"
```

```
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSDataPipeline_PowerUser

Deskripsi: Menyediakan akses penuh ke Data Pipeline, akses daftar untuk peran S3, DynamoDB, Redshift, RDS, SNS, dan IAM, dan akses PassRole untuk Peran default.

`AWSDataPipeline_PowerUser`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDataPipeline_PowerUser` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 19 Januari 2017, 23:16 UTC
- Waktu telah diedit: 17 Agustus 2017, 18:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataPipeline_PowerUser`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "s3:List*",
        "dynamodb:DescribeTable",
        "rds:DescribeDBInstances",
        "rds:DescribeDBSecurityGroups",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSecurityGroups",
        "sns:ListTopics",
        "iam:ListRoles",
        "iam:GetRolePolicy",
        "iam:GetInstanceProfile",
        "iam:ListInstanceProfiles",
        "datapipeline:*"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Action" : "iam:PassRole",
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/DataPipelineDefaultResourceRole",
        "arn:aws:iam::*:role/DataPipelineDefaultRole"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSDataSyncDiscoveryServiceRolePolicy

Deskripsi: Memungkinkan DataSync Discovery untuk berintegrasi dengan AWS layanan lain atas nama Anda.

`AWSDataSyncDiscoveryServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 20 Maret 2023, 22:19 UTC
- Waktu telah diedit: 20 Maret 2023, 22:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDataSyncDiscoveryServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : [
        "arn:*:secretsmanager:*:*:secret:datasync!*"
      ],
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "datasync",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream"
      ],
      "Resource" : [
        "arn:*:logs:*:*:log-group:/aws/datasync*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:*:logs:*:*:log-group:/aws/datasync:log-stream:*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSDataSyncFullAccess

Deskripsi: Menyediakan akses penuh AWS DataSync dan akses minimal ke dependensinya

`AWSDataSyncFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDataSyncFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 Januari 2019, 19:40 UTC
- Waktu yang telah diedit: 20 Mei 2025, 19:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataSyncFullAccess`

Versi kebijakan

Versi kebijakan: v10 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin dengan hak istimewa paling sedikit

AWSDataSyncReadOnlyAccess

Deskripsi: Menyediakan akses hanya-baca ke AWS DataSync

`AWSDataSyncReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDataSyncReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 Januari 2019, 19:18 UTC
- Waktu yang telah diedit: 30 Juni 2020, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataSyncReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "datasync:Describe*",
        "datasync:List*",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets",
        "fsx:DescribeFileSystems",
        "iam:GetRole",
        "iam:ListRoles",
        "logs:DescribeLogGroups",
        "logs:DescribeResourcePolicies",
        "s3:ListAllMyBuckets",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSDataSyncServiceRolePolicy

Deskripsi: Memungkinkan DataSync untuk berintegrasi dengan AWS layanan lain atas nama Anda

`AWSDataSyncServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 09 Oktober 2024, 17:45 UTC
- Waktu telah diedit: April 15, 2025, 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDataSyncServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSDeadlineCloud-FleetWorker

Deskripsi: Menyediakan pekerja AWS Deadline Cloud dengan akses untuk menjalankan tugas di pertanian.

`AWSDeadlineCloud-FleetWorker`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDeadlineCloud-FleetWorker` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 April 2024, 17:21 UTC
- Waktu yang telah diedit: April 01, 2024, 17:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeadlineCloud-FleetWorker`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "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}"
        }
```

```
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSDeadlineCloud-UserAccessFarms

Deskripsi: Menyediakan akses workstation pengguna ke AWS Deadline Cloud farm dengan izin Read-Only terbatas untuk memanggil layanan lain yang diperlukan. Lampirkan kebijakan ini ke peran pengguna yang terkait dengan studio Anda.

`AWSDeadlineCloud-UserAccessFarms`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDeadlineCloud-UserAccessFarms` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 April 2024, 16:54 UTC
- Waktu yang telah diedit: 07 Oktober 2024, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeadlineCloud-UserAccessFarms`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSDeadlineCloud-UserAccessFleets

Deskripsi: Menyediakan akses workstation pengguna ke armada AWS Deadline Cloud dengan izin Read-Only terbatas untuk memanggil layanan lain yang diperlukan. Lampirkan kebijakan ini ke peran pengguna yang terkait dengan studio Anda.

`AWSDeadlineCloud-UserAccessFleets`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDeadlineCloud-UserAccessFleets` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 April 2024, 17:01 UTC

- Waktu yang telah diedit: 01 April 2024, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeadlineCloud-UserAccessFleets`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSDeadlineCloud-UserAccessJobs

Deskripsi: Menyediakan akses workstation pengguna ke pekerjaan AWS Deadline Cloud dengan izin Read-Only terbatas untuk memanggil layanan lain yang diperlukan. Lampirkan kebijakan ini ke peran pengguna yang terkait dengan studio Anda.

`AWSDeadlineCloud-UserAccessJobs`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDeadlineCloud-UserAccessJobs` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 April 2024, 17:05 UTC
- Waktu telah diedit: 07 Oktober 2024, 18:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeadlineCloud-UserAccessJobs`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSDeadlineCloud-UserAccessQueues

Deskripsi: Menyediakan akses workstation pengguna ke antrian AWS Deadline Cloud dengan izin Read-Only terbatas untuk memanggil layanan lain yang diperlukan. Lampirkan kebijakan ini ke peran pengguna yang terkait dengan studio Anda.

`AWSDeadlineCloud-UserAccessQueues`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDeadlineCloud-UserAccessQueues` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 April 2024, 17:10 UTC
- Waktu telah diedit: 07 Oktober 2024, 18:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeadlineCloud-UserAccessQueues`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "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}"
```

```
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSDeadlineCloud-WorkerHost

Deskripsi: Menyediakan akses bagi host pekerja AWS Deadline Cloud untuk bergabung dengan armada di peternakan.

`AWSDeadlineCloud-WorkerHost`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDeadlineCloud-WorkerHost` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 April 2024, 17:28 UTC
- Waktu yang telah diedit: 30 April 2025, 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeadlineCloud-WorkerHost`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSDeepLensLambdaFunctionAccessPolicy

Deskripsi: Kebijakan ini menetapkan izin yang diperlukan oleh fungsi lambda DeepLens Administratif yang berjalan di perangkat DeepLens

`AWSDeepLensLambdaFunctionAccessPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDeepLensLambdaFunctionAccessPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 November 2017, 15:47 UTC
- Waktu yang telah diedit: 11 Juni 2019, 23:11 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepLensLambdaFunctionAccessPolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DeepLensS3ObjectAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::deeplens*/*",
        "arn:aws:s3:::deeplens*"
      ]
    },
    {
      "Sid" : "DeepLensGreenGrassCloudWatchAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents",
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/greengrass/*"
    },
    {
      "Sid" : "DeepLensAccess",
      "Effect" : "Allow",
      "Action" : [
        "deeplens:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
```

```
      "Sid" : "DeepLensKinesisVideoAccess",
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:DescribeStream",
        "kinesisvideo:CreateStream",
        "kinesisvideo:GetDataEndpoint",
        "kinesisvideo:PutMedia"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSDeepLensServiceRolePolicy

Deskripsi: Memberikan AWS DeepLens akses ke Layanan AWS, sumber daya, dan peran yang dibutuhkan oleh DeepLens dan dependensinya termasuk IoT, S3, dan Lambda. GreenGrass AWS

`AWSDeepLensServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDeepLensServiceRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 29 November 2017, 15:46 UTC
- Waktu yang telah diedit: 25 September 2019, 19:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDeepLensServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DeepLensIoTThingAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateThing",
        "iot:DeleteThing",
        "iot:DeleteThingShadow",
        "iot:DescribeThing",
        "iot:GetThingShadow",
        "iot:UpdateThing",
        "iot:UpdateThingShadow"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/deeplens*"
      ]
    },
    {
      "Sid" : "DeepLensIoTCertificateAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:AttachThingPrincipal",
        "iot:DetachThingPrincipal",
        "iot:UpdateCertificate",
        "iot:DeleteCertificate",
        "iot:DetachPrincipalPolicy"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/deeplens*",
        "arn:aws:iot:*:*:cert/*"
      ]
```

```
    },
    {
      "Sid" : "DeepLensIoTCreateCertificateAndPolicyAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateKeysAndCertificate",
        "iot:CreatePolicy",
        "iot:CreatePolicyVersion"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DeepLensIoTAttachCertificatePolicyAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:AttachPrincipalPolicy"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:policy/deeplens*",
        "arn:aws:iot:*:*:cert/*"
      ]
    },
    {
      "Sid" : "DeepLensIoTDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:GetThingShadow",
        "iot:UpdateThingShadow"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/deeplens*"
      ]
    },
    {
      "Sid" : "DeepLensIoTEndpointAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:DescribeEndpoint"
      ],
      "Resource" : [
        "*"
      ]
```

```
    },
    {
      "Sid" : "DeepLensAccess",
      "Effect" : "Allow",
      "Action" : [
        "deeplens:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DeepLensS3ObjectAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::deeplens*"
      ]
    },
    {
      "Sid" : "DeepLensS3Buckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteBucket",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::deeplens*"
      ]
    },
    {
      "Sid" : "DeepLensCreateS3Buckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DeepLensIAMPassRoleAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "greengrass.amazonaws.com",
            "sagemaker.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DeepLensIAMLambdaPassRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSDeepLens*",
        "arn:aws:iam::*:role/service-role/AWSDeepLens*"
      ],
      "Condition" : {
        "StringEqualsIfExists" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DeepLensGreenGrassAccess",
      "Effect" : "Allow",
      "Action" : [
        "greengrass:AssociateRoleToGroup",
        "greengrass:AssociateServiceRoleToAccount",
        "greengrass:CreateResourceDefinition",
        "greengrass:CreateResourceDefinitionVersion",
        "greengrass:CreateCoreDefinition",
        "greengrass:CreateCoreDefinitionVersion",
        "greengrass:CreateDeployment",
        "greengrass:CreateFunctionDefinition",
```

```
        "greengrass:CreateFunctionDefinitionVersion",
        "greengrass:CreateGroup",
        "greengrass:CreateGroupCertificateAuthority",
        "greengrass:CreateGroupVersion",
        "greengrass:CreateLoggerDefinition",
        "greengrass:CreateLoggerDefinitionVersion",
        "greengrass:CreateSubscriptionDefinition",
        "greengrass:CreateSubscriptionDefinitionVersion",
        "greengrass:DeleteCoreDefinition",
        "greengrass:DeleteFunctionDefinition",
        "greengrass:DeleteGroup",
        "greengrass:DeleteLoggerDefinition",
        "greengrass:DeleteSubscriptionDefinition",
        "greengrass:DisassociateRoleFromGroup",
        "greengrass:DisassociateServiceRoleFromAccount",
        "greengrass:GetAssociatedRole",
        "greengrass:GetConnectivityInfo",
        "greengrass:GetCoreDefinition",
        "greengrass:GetCoreDefinitionVersion",
        "greengrass:GetDeploymentStatus",
        "greengrass:GetDeviceDefinition",
        "greengrass:GetDeviceDefinitionVersion",
        "greengrass:GetFunctionDefinition",
        "greengrass:GetFunctionDefinitionVersion",
        "greengrass:GetGroup",
        "greengrass:GetGroupCertificateAuthority",
        "greengrass:GetGroupCertificateConfiguration",
        "greengrass:GetGroupVersion",
        "greengrass:GetLoggerDefinition",
        "greengrass:GetLoggerDefinitionVersion",
        "greengrass:GetResourceDefinition",
        "greengrass:GetServiceRoleForAccount",
        "greengrass:GetSubscriptionDefinition",
        "greengrass:GetSubscriptionDefinitionVersion",
        "greengrass:ListCoreDefinitionVersions",
        "greengrass:ListCoreDefinitions",
        "greengrass:ListDeployments",
        "greengrass:ListDeviceDefinitionVersions",
        "greengrass:ListDeviceDefinitions",
        "greengrass:ListFunctionDefinitionVersions",
        "greengrass:ListFunctionDefinitions",
        "greengrass:ListGroupCertificateAuthorities",
        "greengrass:ListGroupVersions",
        "greengrass:ListGroups",
```

```
        "greengrass:ListLoggerDefinitionVersions",
        "greengrass:ListLoggerDefinitions",
        "greengrass:ListSubscriptionDefinitionVersions",
        "greengrass:ListSubscriptionDefinitions",
        "greengrass:ResetDeployments",
        "greengrass:UpdateConnectivityInfo",
        "greengrass:UpdateCoreDefinition",
        "greengrass:UpdateDeviceDefinition",
        "greengrass:UpdateFunctionDefinition",
        "greengrass:UpdateGroup",
        "greengrass:UpdateGroupCertificateConfiguration",
        "greengrass:UpdateLoggerDefinition",
        "greengrass:UpdateSubscriptionDefinition",
        "greengrass:UpdateResourceDefinition"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DeepLensLambdaAdminFunctionAccess",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:ListFunctions",
        "lambda:ListVersionsByFunction",
        "lambda:PublishVersion",
        "lambda:UpdateFunctionCode",
        "lambda:UpdateFunctionConfiguration"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:deeplens*"
      ]
    },
    {
      "Sid" : "DeepLensLambdaUsersFunctionAccess",
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:ListFunctions",
```

```
        "lambda:ListVersionsByFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*"
      ]
    },
    {
      "Sid" : "DeepLensSageMakerWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateTrainingJob",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:StopTrainingJob"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-job/deeplens*"
      ]
    },
    {
      "Sid" : "DeepLensSageMakerReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeTrainingJob"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-job/*"
      ]
    },
    {
      "Sid" : "DeepLensKinesisVideoStreamAccess",
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:CreateStream",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:DeleteStream"
      ],
      "Resource" : [
        "arn:aws:kinesisvideo:*:*:stream/deeplens*/*"
      ]
    },
    {
      "Sid" : "DeepLensKinesisVideoEndpointAccess",
      "Effect" : "Allow",
      "Action" : [
```

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSDeepRacerAccountAdminAccess

Deskripsi: akses DeepRacer admin ke semua tindakan termasuk beralih antara mode multipengguna dan pengguna tunggal.

`AWSDeepRacerAccountAdminAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDeepRacerAccountAdminAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 Oktober 2021 01:27 UTC
- Waktu yang telah diedit: 28 Oktober 2021, 01:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerAccountAdminAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DeepRacerAdminAccessStatement",
      "Effect" : "Allow",
      "Action" : [
        "deepracer:*"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "Null" : {
          "deepracer:UserToken" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSDeepRacerCloudFormationAccessPolicy

Deskripsi: Memungkinkan CloudFormation untuk membuat dan mengelola AWS tumpukan dan sumber daya atas nama Anda.

`AWSDeepRacerCloudFormationAccessPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDeepRacerCloudFormationAccessPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 Februari 2019, 21:59 UTC
- Waktu yang telah diedit: 14 Juni 2019, 17:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerCloudFormationAccessPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AttachInternetGateway",
        "ec2:AssociateRouteTable",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
```

```
        "ec2:CreateInternetGateway",
        "ec2:CreateNatGateway",
        "ec2:CreateNetworkAcl",
        "ec2:CreateNetworkAclEntry",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateTags",
        "ec2:CreateVpc",
        "ec2:CreateVpcEndpoint",
        "ec2:DeleteInternetGateway",
        "ec2:DeleteNatGateway",
        "ec2:DeleteNetworkAcl",
        "ec2:DeleteNetworkAclEntry",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteSubnet",
        "ec2:DeleteTags",
        "ec2:DeleteVpc",
        "ec2:DeleteVpcEndpoints",
        "ec2:DescribeAddresses",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ec2:DetachInternetGateway",
        "ec2:DisassociateRouteTable",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:ReleaseAddress",
        "ec2:ReplaceNetworkAclAssociation",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/AWSDeepRacerLambdaAccessRole",
      "Condition" : {
        "StringLikeIfExists" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:GetFunction",
        "lambda:DeleteFunction",
        "lambda:TagResource",
        "lambda:UpdateFunctionCode"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*DeepRacer*",
        "arn:aws:lambda:*:*:function:*Deepracer*",
        "arn:aws:lambda:*:*:function:*deepracer*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketPolicy",
        "s3:CreateBucket",
        "s3:ListBucket",
        "s3:GetBucketAcl",
        "s3:DeleteBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::*DeepRacer*",
        "arn:aws:s3:::*Deepracer*",
        "arn:aws:s3:::*deepracer*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "robomaker:CreateSimulationApplication",
        "robomaker:CreateSimulationApplicationVersion",
        "robomaker:DeleteSimulationApplication",
        "robomaker:DescribeSimulationApplication",
        "robomaker:ListSimulationApplications",
        "robomaker:TagResource",
        "robomaker:UpdateSimulationApplication"
      ],
      "Resource" : [
        "arn:aws:robomaker:*:*:/createSimulationApplication",
        "arn:aws:robomaker:*:*:simulation-application/deepracer*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSDeepRacerDefaultMultiUserAccess

Deskripsi: Akses pengguna DeepRacer MultiUser default untuk menggunakan deepracer dalam mode multi-pengguna

`AWSDeepRacerDefaultMultiUserAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDeepRacerDefaultMultiUserAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 Oktober 2021 01:27 UTC

- Waktu yang telah diedit: 28 Oktober 2021, 01:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerDefaultMultiUserAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "deepracer:Add*",
        "deepracer:Remove*",
        "deepracer:Create*",
        "deepracer:Perform*",
        "deepracer:Clone*",
        "deepracer:Get*",
        "deepracer:List*",
        "deepracer:Edit*",
        "deepracer:Start*",
        "deepracer:Set*",
        "deepracer:Update*",
        "deepracer:Delete*",
        "deepracer:Stop*",
        "deepracer:Import*",
        "deepracer:Tag*",
        "deepracer:Untag*"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "Null" : {
```

```
          "deepracer:UserToken" : "false"
        },
        "Bool" : {
          "deepracer:MultiUser" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "deepracer:GetAccountConfig",
        "deepracer:GetTrack",
        "deepracer:ListTracks",
        "deepracer:TestRewardFunction"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "deepracer:Admin*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSDeepRacerFullAccess

Deskripsi: Menyediakan akses penuh ke AWS DeepRacer. Juga menyediakan akses pilih ke layanan terkait (misalnya, S3).

`AWSDeepRacerFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDeepRacerFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 05 Oktober 2020, 22:03 UTC
- Waktu yang telah diedit: 05 Oktober 2020, 22:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetBucketPolicy",
        "s3:PutBucketPolicy",
        "s3:ListBucket",
        "s3:GetBucketAcl",
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetObjectAcl",
        "s3:GetBucketLocation"
      ],
      "Resource" : [
        "arn:aws:s3:::*DeepRacer*",
        "arn:aws:s3:::*Deepracer*",
        "arn:aws:s3:::*deepracer*",
        "arn:aws:s3:::dr-*",
        "arn:aws:s3:::*DeepRacer*/*",
        "arn:aws:s3:::*Deepracer*/*",
        "arn:aws:s3:::*deepracer*/*",
        "arn:aws:s3:::dr-*/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSDeepRacerRoboMakerAccessPolicy

Deskripsi: Memungkinkan RoboMaker untuk membuat sumber daya yang diperlukan dan AWS layanan panggilan atas nama Anda.

`AWSDeepRacerRoboMakerAccessPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDeepRacerRoboMakerAccessPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 Februari 2019, 21:59 UTC
- Waktu yang telah diedit: 28 Februari 2019, 21:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerRoboMakerAccessPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "robomaker:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
```

```
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/robomaker/SimulationJobs",
        "arn:aws:logs:*:*:log-group:/aws/robomaker/SimulationJobs:log-stream:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*DeepRacer*",
        "arn:aws:s3:::*Deepracer*",
        "arn:aws:s3:::*deepracer*",
        "arn:aws:s3:::dr-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/DeepRacer" : "true"
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:CreateStream",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:GetDataEndpoint",
        "kinesisvideo:PutMedia",
        "kinesisvideo:TagStream"
      ],
      "Resource" : [
        "arn:aws:kinesisvideo:*:*:stream/dr-*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSDeepRacerServiceRolePolicy

Deskripsi: Memungkinkan DeepRacer untuk membuat sumber daya yang diperlukan dan AWS layanan panggilan atas nama Anda.

`AWSDeepRacerServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDeepRacerServiceRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan

- Waktu pembuatan: 28 Februari 2019, 21:58 UTC
- Waktu yang telah diedit: 12 Juni 2019, 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDeepRacerServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "deepracer:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "robomaker:*",
        "sagemaker:*",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStackResource",
```

```
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DetectStackDrift",
        "cloudformation:DescribeStackDriftDetectionStatus",
        "cloudformation:DescribeStackResourceDrifts"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "robomaker.amazonaws.com"
        }
      },
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSDeepRacer*",
        "arn:aws:iam::*:role/service-role/AWSDeepRacer*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
```

```
        "lambda:DeleteFunction",
        "lambda:GetFunction",
        "lambda:InvokeFunction",
        "lambda:UpdateFunctionCode"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*DeepRacer*",
        "arn:aws:lambda:*:*:function:*Deepracer*",
        "arn:aws:lambda:*:*:function:*deepracer*",
        "arn:aws:lambda:*:*:function:*dr-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetBucketLocation",
        "s3:DeleteObject",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutBucketPolicy",
        "s3:GetBucketAcl"
      ],
      "Resource" : [
        "arn:aws:s3:::*DeepRacer*",
        "arn:aws:s3:::*Deepracer*",
        "arn:aws:s3:::*deepracer*",
        "arn:aws:s3:::dr-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/DeepRacer" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "kinesisvideo:CreateStream",
        "kinesisvideo:DeleteStream",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:GetDataEndpoint",
        "kinesisvideo:GetHLSStreamingSessionURL",
        "kinesisvideo:GetMedia",
        "kinesisvideo:PutMedia",
        "kinesisvideo:TagStream"
      ],
      "Resource" : [
        "arn:aws:kinesisvideo:*:*:stream/dr-*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSDenyAll

Deskripsi: Tolak semua akses.

`AWSDenyAll`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDenyAll` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Mei 2019 22:36 UTC
- Waktu telah diedit: 18 Desember 2023, 16:42 UTC

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

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSDeviceFarmFullAccess

Deskripsi: Menyediakan akses penuh ke semua operasi AWS Device Farm.

`AWSDeviceFarmFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDeviceFarmFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 13 Juli 2015, 16:37 UTC
- Waktu telah diedit: 13 Juli 2015, 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeviceFarmFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSDeviceFarmServiceRolePolicy

Deskripsi: Berikan izin ke AWS Device Farm untuk memanggil EC2 Jaringan APIs atas nama Anda.

`AWSDeviceFarmServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 20 September 2022, 21:02 UTC
- Waktu yang telah diedit: 20 September 2022, 21.02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDeviceFarmServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AWSDeviceFarmManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSDeviceFarmManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSDeviceFarmManaged" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSDeviceFarmTestGridServiceRolePolicy

Deskripsi: Berikan izin ke AWS Device Farm untuk menelepon EC2 APIs atas nama Anda.

`AWSDeviceFarmTestGridServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 26 Mei 2021 22:01 UTC
- Waktu yang telah diedit: 26 Mei 2021, 22:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDeviceFarmTestGridServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AWSDeviceFarmManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface"
```

```
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSDeviceFarmManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSDeviceFarmManaged" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSDirectConnectFullAccess

Deskripsi: Menyediakan akses penuh ke AWS Direct Connect melalui file AWS Management Console.

`AWSDirectConnectFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDirectConnectFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu yang telah diedit: 30 April 2019, 15:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectConnectFullAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "directconnect:*",
        "ec2:DescribeVpnGateways",
        "ec2:DescribeTransitGateways"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSDirectConnectReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke AWS Direct Connect melalui file AWS Management Console.

`AWSDirectConnectReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDirectConnectReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu yang telah diedit: 18 Mei 2020, 18:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectConnectReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "directconnect:Describe*",
        "directconnect:List*",
        "ec2:DescribeVpnGateways",
        "ec2:DescribeTransitGateways"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSDirectConnectServiceRolePolicy

Deskripsi: Menyediakan izin AWS Direct Connect untuk membuat dan mengelola AWS sumber daya atas nama Anda.

`AWSDirectConnectServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 14 Januari 2021, 18:35 UTC
- Waktu yang telah diedit: 14 Januari 2021, 18.35 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDirectConnectServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:ListSecretVersionIds",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:*directconnect*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSDirectoryServiceDataFullAccess

Deskripsi: Menyediakan akses penuh ke AWS Directory Service Data.

`AWSDirectoryServiceDataFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDirectoryServiceDataFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 September 2024, 21:45 UTC
- Waktu yang telah diedit: 18 September 2024, 21:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectoryServiceDataFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSDirectoryServiceDataReadOnlyAccess

Deskripsi: Menyediakan akses read-only ke AWS Directory Service Data

`AWSDirectoryServiceDataReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDirectoryServiceDataReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 September 2024, 22:00 UTC
- Waktu yang telah diedit: September 18, 2024, 22:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectoryServiceDataReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSDirectoryServiceFullAccess

Deskripsi: Menyediakan akses penuh ke AWS Directory Service.

`AWSDirectoryServiceFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDirectoryServiceFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu yang telah diedit: 02 April 2024, 20:38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectoryServiceFullAccess`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSDirectoryServiceReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke AWS Directory Service.

`AWSDirectoryServiceReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDirectoryServiceReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu yang telah diedit: 25 September 2018, 21:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectoryServiceReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ds:Check*",
        "ds:Describe*",
        "ds:Get*",
        "ds:List*",
        "ds:Verify*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "sns:ListTopics",
        "sns:GetTopicAttributes",
```

```
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSDiscoveryContinuousExportFirehosePolicy

Deskripsi: Menyediakan akses tulis ke AWS sumber daya yang diperlukan untuk AWS Discovery Continuous Export

`AWSDiscoveryContinuousExportFirehosePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDiscoveryContinuousExportFirehosePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 09 Agustus 2018, 18:29 UTC
- Waktu yang telah diedit: 08 Juni 2021, 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDiscoveryContinuousExportFirehosePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:GetTableVersions"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-application-discovery-service-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/application-discovery-service/firehose:log-
stream:*"
      ]
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSDMSFleetAdvisorServiceRolePolicy

Deskripsi: Memungkinkan DMS Fleet Advisor untuk mengelola CloudWatch metrik atas nama Anda.

`AWSDMSFleetAdvisorServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 06 Maret 2023, 09:10 UTC
- Waktu telah diedit: 06 Maret 2023, 09:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDMSFleetAdvisorServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : "cloudwatch:PutMetricData",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "cloudwatch:namespace" : "AWS/DMS/FleetAdvisor"
      }
    }
  }
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSDMSServerlessServiceRolePolicy

Deskripsi: Memberikan izin AWS DMS Tanpa Server untuk membuat dan mengelola sumber daya DMS di akun Anda atas nama Anda

`AWSDMSServerlessServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 18 Mei 2023, 20:28 UTC
- Waktu telah diedit: 07 Februari 2025, 17:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDMSServerlessServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "id0",
      "Effect" : "Allow",
      "Action" : [
        "dms:CreateReplicationInstance",
        "dms:CreateReplicationTask"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "dms:req-tag/ResourceCreatedBy" : "DMSServerless"
        }
      }
    },
    {
      "Sid" : "id1",
      "Effect" : "Allow",
      "Action" : [
        "dms:DescribeReplicationInstances",
```

```
        "dms:DescribeReplicationTasks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "id2",
      "Effect" : "Allow",
      "Action" : [
        "dms:StartReplicationTask",
        "dms:StopReplicationTask",
        "dms: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-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "id5",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketPolicy",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::dms-serverless-premigration-results-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "id6",
      "Effect" : "Allow",
      "Action" : [
        "dms:StartReplicationTaskAssessmentRun"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "aws:ResourceTag/ResourceCreatedBy" : "DMSServerless"
        }
      }
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSEC2CapacityReservationFleetRolePolicy

Deskripsi: Memungkinkan layanan EC2 CapacityReservation Armada untuk mengelola Reservasi Kapasitas

`AWSEC2CapacityReservationFleetRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 29 September 2021 14:43 UTC
- Waktu telah diedit: 03 Maret 2025, 23:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2CapacityReservationFleetRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeInstances"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateCapacityReservation",
        "ec2:CancelCapacityReservation",
        "ec2:ModifyCapacityReservation"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:capacity-reservation/*"
      ],
      "Condition" : {
        "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"
        }
      }
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin dengan hak istimewa paling sedikit

AWSEC2FleetServiceRolePolicy

Deskripsi: Memungkinkan EC2 Armada untuk meluncurkan dan mengelola instance.

`AWSEC2FleetServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 21 Maret 2018, 00:08 UTC
- Waktu yang telah diedit: 04 Mei 2020, 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2FleetServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSEC2SpotFleetServiceRolePolicy

Deskripsi: Memungkinkan Armada EC2 Spot untuk meluncurkan dan mengelola instance armada spot

`AWSEC2SpotFleetServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 23 Oktober 2017, 19:13 UTC
- Waktu yang telah diedit: 16 Maret 2020, 19:16 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2SpotFleetServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSubnets",
        "ec2:RequestSpotInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:spot-instances-request/*",
        "arn:aws:ec2:*:*:spot-fleet-request/*",
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:ec2spot:fleet-request-id" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterTargets"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:*/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSEC2SpotServiceRolePolicy

Deskripsi: Memungkinkan EC2 Spot untuk meluncurkan dan mengelola instans spot

`AWSEC2SpotServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 18 September 2017, 18:51 UTC
- Waktu diedit: 12 Desember 2018, 00:13 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2SpotServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSEC2VssSnapshotPolicy

Deskripsi: Kebijakan ini dilampirkan ke peran IAM yang dilampirkan ke Instans Amazon EC2 Windows Anda untuk mengaktifkan solusi Amazon EC2 VSS untuk membuat dan menambahkan tag ke Gambar Mesin Amazon (AMI) dan Snapshot EBS.

`AWSEC2VssSnapshotPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSEC2VssSnapshotPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Maret 2024, 16:32 UTC
- Waktu telah diedit: 20 November 2024, 17:44 UTC
- ARN: `arn:aws:iam::aws:policy/AWSEC2VssSnapshotPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSECRPullThroughCache_ServiceRolePolicy

Deskripsi: Memungkinkan akses ke AWS layanan dan sumber daya yang digunakan atau dikelola oleh AWS ECR pull through cache

`AWSECRPullThroughCache_ServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 26 November 2021 21:51 UTC
- Waktu telah diedit: 06 Maret 2025, 21:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSECRPullThroughCache_ServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElasticBeanstalkCustomPlatformforEC2Role

Deskripsi: Berikan instans di izin lingkungan pembuat platform khusus Anda untuk meluncurkan EC2 instans, membuat snapshot EBS dan AMI, mengalirkan log ke Amazon CloudWatch Log, dan menyimpan artefak di Amazon S3.

`AWSElasticBeanstalkCustomPlatformforEC2Role`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticBeanstalkCustomPlatformforEC2Role` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 21 Februari 2017, 22:50 UTC
- Waktu telah diedit: 21 Februari 2017, 22:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkCustomPlatformforEC2Role`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2Access",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CopyImage",
        "ec2:CreateImage",
```

```
        "ec2:CreateKeypair",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSnapshot",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:DeleteKeypair",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteSnapshot",
        "ec2:DeleteVolume",
        "ec2:DeregisterImage",
        "ec2:DescribeImageAttribute",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeRegions",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVolumes",
        "ec2:DetachVolume",
        "ec2:GetPasswordData",
        "ec2:ModifyImageAttribute",
        "ec2:ModifyInstanceAttribute",
        "ec2:ModifySnapshotAttribute",
        "ec2:RegisterImage",
        "ec2:RunInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "BucketAccess",
      "Action" : [
        "s3:Get*",
        "s3:List*",
        "s3:PutObject"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:s3:::elasticbeanstalk-*",
        "arn:aws:s3:::elasticbeanstalk-*/*"
      ]
```

```
    },
    {
      "Sid" : "CloudWatchLogsAccess",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/platform/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElasticBeanstalkEnhancedHealth

Keterangan: Kebijakan Layanan AWS Elastic Beanstalk untuk sistem Pemantauan Kesehatan

`AWSElasticBeanstalkEnhancedHealth`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticBeanstalkEnhancedHealth` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 08 Februari 2016, 23:17 UTC
- Waktu yang telah diedit: 09 April 2018, 22:12 UTC

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

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetHealth",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:GetConsoleOutput",
        "ec2:AssociateAddress",
        "ec2:DescribeAddresses",
        "ec2:DescribeSecurityGroups",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeScalingActivities",
        "autoscaling:DescribeNotificationConfigurations",
        "sns:Publish"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*:log-stream:*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElasticBeanstalkMaintenance

Deskripsi: AWS Kebijakan Peran Layanan Elastic Beanstalk yang memberikan izin terbatas untuk memperbarui sumber daya Anda atas nama Anda untuk tujuan pemeliharaan.

`AWSElasticBeanstalkMaintenance`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 11 Januari 2019, 23:22 UTC
- Waktu yang telah diedit: 29 April 2024, 21:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkMaintenance`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy

Deskripsi: Kebijakan ini untuk peran layanan AWS Elastic Beanstalk yang digunakan untuk melakukan pembaruan terkelola lingkungan Elastic Beanstalk. Kebijakan ini tidak boleh dilampirkan pada pengguna atau peran lain. Kebijakan ini memberikan izin luas untuk membuat dan mengelola sumber daya di sejumlah AWS layanan termasuk AutoScaling,, ECS EC2, Elastic Load Balancing dan. CloudFormation Kebijakan ini juga memungkinkan melewati peran IAM apa pun yang dapat digunakan dengan layanan tersebut.

`AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 Maret 2021 22:18 UTC
- Waktu yang telah diedit: 27 Februari 2025, 16:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ElasticBeanstalkPermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticbeanstalk:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowPassRoleToElasticBeanstalkAndDownstreamServices",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "elasticbeanstalk.amazonaws.com",
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn",
            "autoscaling.amazonaws.com",
            "elasticloadbalancing.amazonaws.com",
            "ecs.amazonaws.com",
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAccountLimits",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeLaunchConfigurations",
        "autoscaling:DescribeLoadBalancers",
        "autoscaling:DescribeNotificationConfigurations",
        "autoscaling:DescribeScalingActivities",
```

```
        "autoscaling:DescribeScheduledActions",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "logs:DescribeLogGroups",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeOrderableDBInstanceOptions",
        "sns:ListSubscriptionsByTopic"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EC2BroadOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AssociateAddress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions",
        "ec2:DeleteSecurityGroup",
```

```
        "ec2:DisassociateAddress",
        "ec2:ReleaseAddress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2RunInstancesOperationPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ec2:LaunchTemplate" : "arn:aws:ec2:*:*:launch-template/*"
        }
      }
    },
    {
      "Sid" : "EC2TerminateInstancesOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" : [
            "arn:aws:cloudformation:*:*:stack/awseb-e-*",
            "arn:aws:cloudformation:*:*:stack/eb-*"
          ]
        }
      }
    },
    {
      "Sid" : "ECSBroadOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecs:CreateCluster",
        "ecs:DescribeClusters",
        "ecs:RegisterTaskDefinition"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "ECSDeleteClusterOperationPermissions",
      "Effect" : "Allow",
      "Action" : "ecs:DeleteCluster",
      "Resource" : "arn:aws:ecs:*:*:cluster/awseb-*"
    },
    {
      "Sid" : "ASGOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:AttachInstances",
        "autoscaling:CreateAutoScalingGroup",
        "autoscaling:CreateLaunchConfiguration",
        "autoscaling:CreateOrUpdateTags",
        "autoscaling:DeleteLaunchConfiguration",
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:DeleteScheduledAction",
        "autoscaling:DetachInstances",
        "autoscaling:DeletePolicy",
        "autoscaling:PutScalingPolicy",
        "autoscaling:PutScheduledUpdateGroupAction",
        "autoscaling:PutNotificationConfiguration",
        "autoscaling:ResumeProcesses",
        "autoscaling:SetDesiredCapacity",
        "autoscaling:SuspendProcesses",
        "autoscaling:TerminateInstanceInAutoScalingGroup",
        "autoscaling:UpdateAutoScalingGroup"
      ],
      "Resource" : [
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/awseb-e-
*",
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/eb-*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/awseb-e-*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/eb-*"
      ]
    },
    {
      "Sid" : "CFNOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:*"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awseb-*",
```

```
        "arn:aws:cloudformation:*:*:stack/eb-*"
      ]
    },
    {
      "Sid" : "ELBOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
        "elasticloadbalancing:ConfigureHealthCheck",
        "elasticloadbalancing:CreateLoadBalancer",
        "elasticloadbalancing:DeleteLoadBalancer",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:RegisterTargets"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:targetgroup/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:targetgroup/eb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/eb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/*/awseb-*/*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/*/eb-*/*"
      ]
    },
    {
      "Sid" : "CWLogsOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:DeleteLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*"
    },
    {
      "Sid" : "S3ObjectOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectVersion",
```

```
        "s3:GetObjectVersionAcl",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:PutObjectVersionAcl"
      ],
      "Resource" : "arn:aws:s3:::elasticbeanstalk-*/*"
    },
    {
      "Sid" : "S3BucketOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:GetBucketPolicy",
        "s3:ListBucket",
        "s3:PutBucketPolicy"
      ],
      "Resource" : "arn:aws:s3:::elasticbeanstalk-*"
    },
    {
      "Sid" : "SNSOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:GetTopicAttributes",
        "sns:SetTopicAttributes",
        "sns:Subscribe"
      ],
      "Resource" : "arn:aws:sns:*:*:ElasticBeanstalkNotifications-*"
    },
    {
      "Sid" : "SQSOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:awseb-e-*",
        "arn:aws:sqs:*:*:eb-*"
      ]
    },
    {
      "Sid" : "CWPutMetricAlarmOperationPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:awseb-*",
        "arn:aws:cloudwatch:*:*:alarm:eb-*"
      ]
    },
    {
      "Sid" : "AllowECSTagResource",
      "Effect" : "Allow",
      "Action" : [
        "ecs:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ecs:CreateAction" : [
            "CreateCluster",
            "RegisterTaskDefinition"
          ]
        }
      }
    },
    {
      "Sid" : "LaunchTemplateTagPropagationPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:createTags",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateLaunchTemplate",
            "RunInstances"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElasticBeanstalkManagedUpdatesServiceRolePolicy

Deskripsi: AWS Kebijakan Peran Layanan Elastic Beanstalk yang memberikan izin terbatas untuk pembaruan terkelola.

`AWSElasticBeanstalkManagedUpdatesServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 21 November 2019, 22:35 UTC
- Waktu telah diedit: 29 April 2024, 23:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkManagedUpdatesServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElasticBeanstalkMulticontainerDocker

Deskripsi: Berikan instans dalam akses lingkungan Docker multicontainer Anda untuk menggunakan Amazon EC2 Container Service untuk mengelola tugas penerapan container.

`AWSElasticBeanstalkMulticontainerDocker`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticBeanstalkMulticontainerDocker` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 08 Februari 2016, 23:15 UTC
- Waktu telah diedit: 23 Maret 2023, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkMulticontainerDocker`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ECSAccess",
      "Effect" : "Allow",
      "Action" : [
        "ecs:Poll",
        "ecs:StartTask",
        "ecs:StopTask",
        "ecs:DiscoverPollEndpoint",
        "ecs:StartTelemetrySession",
        "ecs:RegisterContainerInstance",
        "ecs:DeregisterContainerInstance",
        "ecs:DescribeContainerInstances",
        "ecs:Submit*",
        "ecs:DescribeTasks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowECSTagResource",
      "Effect" : "Allow",
      "Action" : [
        "ecs:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ecs:CreateAction" : [
            "RegisterContainerInstance",
            "StartTask"
          ]
```

```
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElasticBeanstalkReadOnly

Deskripsi: Memberikan izin hanya-baca. Secara eksplisit memungkinkan operator untuk mendapatkan akses langsung untuk mengambil informasi tentang sumber daya yang terkait dengan aplikasi Elastic Beanstalk AWS .

`AWSElasticBeanstalkReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticBeanstalkReadOnly` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 22 Januari 2021, 19:02 UTC
- Waktu yang telah diedit: 22 Januari 2021, 19:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkReadOnly`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowAPIs",
      "Effect" : "Allow",
      "Action" : [
        "acm:ListCertificates",
        "autoscaling:DescribeAccountLimits",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeLaunchConfigurations",
        "autoscaling:DescribePolicies",
        "autoscaling:DescribeLoadBalancers",
        "autoscaling:DescribeNotificationConfigurations",
        "autoscaling:DescribeScalingActivities",
        "autoscaling:DescribeScheduledActions",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:GetTemplate",
        "cloudformation:ListStackResources",
        "cloudformation:ListStacks",
        "cloudformation:ValidateTemplate",
        "cloudtrail:LookupEvents",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
```

```
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "elasticbeanstalk:Check*",
        "elasticbeanstalk:Describe*",
        "elasticbeanstalk:List*",
        "elasticbeanstalk:RequestEnvironmentInfo",
        "elasticbeanstalk:RetrieveEnvironmentInfo",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeSSLPolicies",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "iam:GetRole",
        "iam:ListAttachedRolePolicies",
        "iam:ListInstanceProfiles",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListServerCertificates",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeOrderableDBInstanceOptions",
        "rds:DescribeDBSnapshots",
        "s3:ListAllMyBuckets",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "sqs:ListQueues"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowS3",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionAcl",
        "s3:GetBucketLocation",
        "s3:GetBucketPolicy",
        "s3:ListBucket"
```

```
      ],
      "Resource" : "arn:aws:s3:::elasticbeanstalk-*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElasticBeanstalkRoleCore

Deskripsi: AWSElastic BeanstalkRoleCore (Peran operasi Elastic Beanstalk) Memungkinkan operasi inti dari lingkungan layanan web.

`AWSElasticBeanstalkRoleCore`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticBeanstalkRoleCore` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 05 Juni 2020, 21:48 UTC
- Waktu yang telah diedit: 30 April 2024, 00:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleCore`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TerminateInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
 "arn:aws:cloudformation:*:*:stack/awseb-e-*"
        }
      }
    },
    {
      "Sid" : "EC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ReleaseAddress",
        "ec2:AllocateAddress",
        "ec2:DisassociateAddress",
        "ec2:AssociateAddress",
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteSecurityGroup",
        "ec2:AuthorizeSecurityGroup*",
        "ec2:RevokeSecurityGroup*",
        "ec2:CreateLaunchTemplate*",
        "ec2:DeleteLaunchTemplate*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LTRunInstances",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : "*",
```

```
      "Condition" : {
        "ArnLike" : {
          "ec2:LaunchTemplate" : "arn:aws:ec2:*:*:launch-template/*"
        }
      }
    },
    {
      "Sid" : "ASG",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:AttachInstances",
        "autoscaling:*LoadBalancer*",
        "autoscaling:*AutoScalingGroup",
        "autoscaling:*LaunchConfiguration",
        "autoscaling:DeleteScheduledAction",
        "autoscaling:DetachInstances",
        "autoscaling:PutNotificationConfiguration",
        "autoscaling:PutScalingPolicy",
        "autoscaling:PutScheduledUpdateGroupAction",
        "autoscaling:ResumeProcesses",
        "autoscaling:SuspendProcesses",
        "autoscaling:*Tags"
      ],
      "Resource" : [
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/awseb-e-
*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/awseb-e-*"
      ]
    },
    {
      "Sid" : "ASGPolicy",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DeletePolicy"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EBSLR",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
```

```
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/elasticbeanstalk.amazonaws.com/
AWSServiceRoleForElasticBeanstalk*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "elasticbeanstalk.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "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"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElasticBeanstalkRoleCWL

Deskripsi: (Peran operasi Elastic Beanstalk) Memungkinkan lingkungan mengelola CloudWatch grup log Amazon Logs.

`AWSElasticBeanstalkRoleCWL`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticBeanstalkRoleCWL` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 05 Juni 2020, 21:49 UTC
- Waktu yang telah diedit: 05 Juni 2020, 21:49 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleCWL`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
        "logs:CreateLogGroup",
        "logs:DeleteLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElasticBeanstalkRoleECS

Deskripsi: (Peran operasi Elastic Beanstalk) Memungkinkan lingkungan Docker multicontainer untuk mengelola cluster Amazon ECS.

`AWSElasticBeanstalkRoleECS`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticBeanstalkRoleECS` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 05 Juni 2020, 21:47 UTC
- Waktu telah diedit: 23 Maret 2023, 22:43 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleECS`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowECS",
      "Effect" : "Allow",
      "Action" : [
        "ecs:CreateCluster",
        "ecs:DeleteCluster",
        "ecs:RegisterTaskDefinition",
        "ecs:DeRegisterTaskDefinition"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowECSTagResource",
      "Effect" : "Allow",
      "Action" : [
        "ecs:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ecs:CreateAction" : [
            "CreateCluster",
            "RegisterTaskDefinition"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElasticBeanstalkRoleRDS

Deskripsi: (Peran operasi Elastic Beanstalk) Memungkinkan lingkungan mengintegrasikan instans Amazon RDS.

`AWSElasticBeanstalkRoleRDS`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticBeanstalkRoleRDS` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 05 Juni 2020, 21:46 UTC
- Waktu yang telah diedit: 05 Juni 2020, 21:46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleRDS`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowRDS",
      "Effect" : "Allow",
      "Action" : [
        "rds:CreateDBSecurityGroup",
        "rds:DeleteDBSecurityGroup",
        "rds:AuthorizeDBSecurityGroupIngress",
        "rds:CreateDBInstance",
        "rds:ModifyDBInstance",
        "rds:DeleteDBInstance"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:secgrp:awseb-e-*",
        "arn:aws:rds:*:*:db:*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElasticBeanstalkRoleSNS

Deskripsi: (Peran operasi Elastic Beanstalk) Memungkinkan lingkungan mengaktifkan integrasi topik Amazon SNS.

`AWSElasticBeanstalkRoleSNS`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticBeanstalkRoleSNS` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 05 Juni 2020, 21:46 UTC
- Waktu yang telah diedit: 05 Juni 2020, 21:46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleSNS`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowBeanstalkManageSNS",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:SetTopicAttributes",
        "sns:DeleteTopic"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:ElasticBeanstalkNotifications-*"
      ]
    },
    {
      "Sid" : "AllowSNSPublish",
      "Effect" : "Allow",
      "Action" : [
        "sns:GetTopicAttributes",
        "sns:Subscribe",
        "sns:Unsubscribe",
        "sns:Publish"
```

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElasticBeanstalkRoleWorkerTier

Deskripsi: (Peran operasi Elastic Beanstalk) Memungkinkan tingkat lingkungan pekerja untuk membuat tabel Amazon DynamoDB dan antrian Amazon SQS.

`AWSElasticBeanstalkRoleWorkerTier`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticBeanstalkRoleWorkerTier` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 05 Juni 2020, 21:43 UTC
- Waktu yang telah diedit: 05 Juni 2020, 21:43 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleWorkerTier`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSQS",
      "Effect" : "Allow",
      "Action" : [
        "sqs:TagQueue",
        "sqs:DeleteQueue",
        "sqs:GetQueueAttributes",
        "sqs:CreateQueue"
      ],
      "Resource" : "arn:aws:sqs:*:*:awseb-e-*"
    },
    {
      "Sid" : "AllowDDB",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:CreateTable",
        "dynamodb:TagResource",
        "dynamodb:DescribeTable",
        "dynamodb:DeleteTable"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/awseb-e-*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElasticBeanstalkService

Deskripsi: Kebijakan ini berada di jalur penghentian. Lihat dokumentasi untuk panduan: https://docs.aws.amazon.com/elasticbeanstalk/ latest/dg/iam -servicerole.html. AWS Kebijakan peran Layanan Elastic Beanstalk yang memberikan izin untuk membuat & mengelola sumber daya (AutoScalingyaitu EC2:,, CloudFormation S3,, ELB, dll.) Atas nama Anda.

`AWSElasticBeanstalkService`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticBeanstalkService` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 11 April 2016, 20:27 UTC
- Waktu yang telah diedit: 10 Mei 2023, 19:29 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkService`

Versi kebijakan

Versi kebijakan: v17 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
        "arn:aws:cloudformation:*:*:stack/awseb-*",
        "arn:aws:cloudformation:*:*:stack/eb-*"
      ]
    },
    {
      "Sid" : "AllowDeleteCloudwatchLogGroups",
      "Effect" : "Allow",
      "Action" : [
        "logs:DeleteLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk*"
      ]
    },
    {
      "Sid" : "AllowECSTagResource",
      "Effect" : "Allow",
      "Action" : [
        "ecs:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ecs:CreateAction" : [
            "CreateCluster",
            "RegisterTaskDefinition"
          ]
        }
      }
    },
    {
      "Sid" : "AllowS3OperationsOnElasticBeanstalkBuckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:*"
      ],
      "Resource" : [
        "arn:aws:s3:::elasticbeanstalk-*",
        "arn:aws:s3:::elasticbeanstalk-*/*"
      ]
    },
    {
      "Sid" : "AllowLaunchTemplateRunInstances",
      "Effect" : "Allow",
```

```
      "Action" : "ec2:RunInstances",
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ec2:LaunchTemplate" : "arn:aws:ec2:*:*:launch-template/*"
        }
      }
    },
    {
      "Sid" : "AllowELBAddTags",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "elasticloadbalancing:CreateAction" : [
            "CreateLoadBalancer"
          ]
        }
      }
    },
    {
      "Sid" : "AllowOperations",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:AttachInstances",
        "autoscaling:CreateAutoScalingGroup",
        "autoscaling:CreateLaunchConfiguration",
        "autoscaling:CreateOrUpdateTags",
        "autoscaling:DeleteLaunchConfiguration",
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:DeleteScheduledAction",
        "autoscaling:DescribeAccountLimits",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeLaunchConfigurations",
        "autoscaling:DescribeLoadBalancers",
        "autoscaling:DescribeNotificationConfigurations",
        "autoscaling:DescribeScalingActivities",
        "autoscaling:DescribeScheduledActions",
        "autoscaling:DetachInstances",
        "autoscaling:DeletePolicy",
```

```
        "autoscaling:PutScalingPolicy",
        "autoscaling:PutScheduledUpdateGroupAction",
        "autoscaling:PutNotificationConfiguration",
        "autoscaling:ResumeProcesses",
        "autoscaling:SetDesiredCapacity",
        "autoscaling:SuspendProcesses",
        "autoscaling:TerminateInstanceInAutoScalingGroup",
        "autoscaling:UpdateAutoScalingGroup",
        "cloudwatch:PutMetricAlarm",
        "ec2:AssociateAddress",
        "ec2:AllocateAddress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeVpcClassicLink",
        "ec2:DisassociateAddress",
        "ec2:ReleaseAddress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:TerminateInstances",
        "ecs:CreateCluster",
        "ecs:DeleteCluster",
        "ecs:DescribeClusters",
        "ecs:RegisterTaskDefinition",
        "elasticbeanstalk:*",
        "elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
```

```
        "elasticloadbalancing:ConfigureHealthCheck",
        "elasticloadbalancing:CreateLoadBalancer",
        "elasticloadbalancing:DeleteLoadBalancer",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:DeregisterTargets",
        "iam:ListRoles",
        "iam:PassRole",
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy",
        "logs:DescribeLogGroups",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeOrderableDBInstanceOptions",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:ListBucket",
        "sns:CreateTopic",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptionsByTopic",
        "sns:Subscribe",
        "sns:SetTopicAttributes",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "codebuild:CreateProject",
        "codebuild:DeleteProject",
        "codebuild:BatchGetBuilds",
        "codebuild:StartBuild"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElasticBeanstalkServiceRolePolicy

Deskripsi: AWS Kebijakan Peran Tertaut Layanan Elastic Beanstalk yang memberikan izin untuk membuat & mengelola sumber daya (AutoScalingyaitu EC2:,, CloudFormation S3,, ELB, dll.) Atas nama Anda.

`AWSElasticBeanstalkServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 13 September 2017, 23:46 UTC
- Waktu yang telah diedit: 06 Juni 2019, 21:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCloudformationReadOperationsOnElasticBeanstalkStacks",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awseb-*",
        "arn:aws:cloudformation:*:*:stack/eb-*"
      ]
    },
    {
      "Sid" : "AllowOperations",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeNotificationConfigurations",
        "autoscaling:DescribeScalingActivities",
        "autoscaling:PutNotificationConfiguration",
        "ec2:DescribeInstanceStatus",
        "ec2:AssociateAddress",
        "ec2:DescribeAddresses",
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeTargetGroups",
        "lambda:GetFunction",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sns:Publish"
      ],
      "Resource" : [
        "*"
```

```
      ]
    },
    {
      "Sid" : "AllowOperationsOnHealthStreamingLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:DeleteLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElasticBeanstalkWebTier

Deskripsi: Berikan instans di lingkungan server web Anda akses untuk mengunggah file log ke Amazon S3.

`AWSElasticBeanstalkWebTier`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticBeanstalkWebTier` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 08 Februari 2016, 23:08 UTC
- Waktu yang telah diedit: 09 September 2020, 19:38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkWebTier`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BucketAccess",
      "Action" : [
        "s3:Get*",
        "s3:List*",
        "s3:PutObject"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:s3:::elasticbeanstalk-*",
        "arn:aws:s3:::elasticbeanstalk-*/*"
      ]
    },
    {
      "Sid" : "XRayAccess",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchLogsAccess",
      "Action" : [
        "logs:PutLogEvents",
        "logs:CreateLogStream",
```

```
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk*"
      ]
    },
    {
      "Sid" : "ElasticBeanstalkHealthAccess",
      "Action" : [
        "elasticbeanstalk:PutInstanceStatistics"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:elasticbeanstalk:*:*:application/*",
        "arn:aws:elasticbeanstalk:*:*:environment/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElasticBeanstalkWorkerTier

Deskripsi: Berikan instans di lingkungan pekerja Anda akses untuk mengunggah file log ke Amazon S3, untuk menggunakan Amazon SQS untuk memantau antrian pekerjaan aplikasi Anda, menggunakan Amazon DynamoDB untuk melakukan pemilihan pemimpin, dan ke Amazon untuk menerbitkan metrik untuk pemantauan kesehatan. CloudWatch

`AWSElasticBeanstalkWorkerTier`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticBeanstalkWorkerTier` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 08 Februari 2016, 23:12 UTC
- Waktu yang telah diedit: September 09, 2020, 19:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkWorkerTier`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MetricsAccess",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "XRayAccess",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
```

```
        "xray:GetSamplingStatisticSummaries"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "QueueAccess",
      "Action" : [
        "sqs:ChangeMessageVisibility",
        "sqs:DeleteMessage",
        "sqs:ReceiveMessage",
        "sqs:SendMessage"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "BucketAccess",
      "Action" : [
        "s3:Get*",
        "s3:List*",
        "s3:PutObject"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:s3:::elasticbeanstalk-*",
        "arn:aws:s3:::elasticbeanstalk-*/*"
      ]
    },
    {
      "Sid" : "DynamoPeriodicTasks",
      "Action" : [
        "dynamodb:BatchGetItem",
        "dynamodb:BatchWriteItem",
        "dynamodb:DeleteItem",
        "dynamodb:GetItem",
        "dynamodb:PutItem",
        "dynamodb:Query",
        "dynamodb:Scan",
        "dynamodb:UpdateItem"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:dynamodb:*:*:table/*-stack-AWSEBWorkerCronLeaderRegistry*"
```

```
      ]
    },
    {
      "Sid" : "CloudWatchLogsAccess",
      "Action" : [
        "logs:PutLogEvents",
        "logs:CreateLogStream"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk*"
      ]
    },
    {
      "Sid" : "ElasticBeanstalkHealthAccess",
      "Action" : [
        "elasticbeanstalk:PutInstanceStatistics"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:elasticbeanstalk:*:*:application/*",
        "arn:aws:elasticbeanstalk:*:*:environment/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElasticDisasterRecoveryAgentInstallationPolicy

Deskripsi: Kebijakan ini memungkinkan penginstalan Agen AWS Replikasi, yang digunakan dengan AWS Elastic Disaster Recovery (DRS) untuk memulihkan server eksternal. AWS Lampirkan kebijakan ini ke pengguna IAM Anda atau peran yang kredensialnya Anda berikan selama langkah instalasi Agen Replikasi. AWS

`AWSElasticDisasterRecoveryAgentInstallationPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticDisasterRecoveryAgentInstallationPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 17 November 2021 10:37 UTC
- Waktu telah diedit: November 27, 2023, 12:38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryAgentInstallationPolicy`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSAgentInstallationPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:GetAgentInstallationAssetsForDrs",
        "drs:SendClientLogsForDrs",
        "drs:SendClientMetricsForDrs",
        "drs:CreateSourceServerForDrs",
        "drs:CreateRecoveryInstanceForDrs",
        "drs:DescribeRecoveryInstances",
        "drs:CreateSourceNetwork"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSAgentInstallationPolicy2",
      "Effect" : "Allow",
      "Action" : "drs:TagResource",
      "Resource" : "arn:aws:drs:*:*:source-server/*",
      "Condition" : {
        "StringEquals" : {
          "drs:CreateAction" : "CreateSourceServerForDrs"
        }
      }
    },
    {
      "Sid" : "DRSAgentInstallationPolicy3",
      "Effect" : "Allow",
      "Action" : "drs:TagResource",
      "Resource" : "arn:aws:drs:*:*:source-server/*",
      "Condition" : {
        "StringEquals" : {
          "drs:CreateAction" : "CreateRecoveryInstanceForDrs"
        }
      }
    },
    {
      "Sid" : "DRSAgentInstallationPolicy4",
      "Effect" : "Allow",
      "Action" : "drs:TagResource",
      "Resource" : "arn:aws:drs:*:*:source-network/*",
      "Condition" : {
        "StringEquals" : {
          "drs:CreateAction" : "CreateSourceNetwork"
        }
      }
    },
    {
      "Sid" : "DRSAgentInstallationPolicy5",
      "Effect" : "Allow",
      "Action" : "drs:IssueAgentCertificateForDrs",
      "Resource" : "arn:aws:drs:*:*:source-server/*"
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElasticDisasterRecoveryAgentPolicy

Deskripsi: Kebijakan ini memungkinkan penggunaan Agen AWS Replikasi, yang digunakan dengan AWS Elastic Disaster Recovery (DRS) untuk memulihkan server sumber. AWS Kami tidak menyarankan Anda melampirkan kebijakan ini ke pengguna atau peran IAM Anda.

`AWSElasticDisasterRecoveryAgentPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticDisasterRecoveryAgentPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 17 November 2021 10:32 UTC
- Waktu telah diedit: 27 November 2023, 13:44 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryAgentPolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSAgentPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:SendAgentMetricsForDrs",
        "drs:SendAgentLogsForDrs",
        "drs:UpdateAgentSourcePropertiesForDrs",
        "drs:UpdateAgentReplicationInfoForDrs",
        "drs:UpdateAgentConversionInfoForDrs",
        "drs:GetAgentCommandForDrs",
        "drs:GetAgentConfirmedResumeInfoForDrs",
        "drs:GetAgentRuntimeConfigurationForDrs",
        "drs:UpdateAgentBacklogForDrs",
        "drs:GetAgentReplicationInfoForDrs",
        "drs:IssueAgentCertificateForDrs"
      ],
      "Resource" : "arn:aws:drs:*:*:source-server/${aws:SourceIdentity}"
    },
    {
      "Sid" : "DRSAgentPolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:GetAgentInstallationAssetsForDrs"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElasticDisasterRecoveryConsoleFullAccess

Deskripsi: Kebijakan ini menyediakan akses penuh ke semua publik APIs AWS Elastic Disaster Recovery (DRS), serta izin untuk membaca kunci KMS, License Manager, Resource Groups, Elastic Load Balancing, IAM, dan informasi. EC2 Lampirkan kebijakan ini ke pengguna atau peran IAM Anda.

`AWSElasticDisasterRecoveryConsoleFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticDisasterRecoveryConsoleFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 17 November 2021 10:46 UTC
- Waktu telah diedit: 12 Januari 2025, 07:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryConsoleFullAccess`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ConsoleFullAccess1",
      "Effect" : "Allow",
      "Action" : [
        "drs:*"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess2",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetEbsDefaultKmsKeyId",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeHosts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess4",
      "Effect" : "Allow",
      "Action" : "license-manager:ListLicenseConfigurations",
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "ConsoleFullAccess5",
      "Effect" : "Allow",
      "Action" : "resource-groups:ListGroups",
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess6",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DescribeLoadBalancers",
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess7",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListInstanceProfiles",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess8",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryConversionServerRole",
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryRecoveryInstanceRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess9",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
```

```
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess10",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions",
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess11",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess12",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
```

```
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess13",
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:GetConsoleOutput",
        "ec2:GetConsoleScreenshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess14",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
```

```
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess15",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess16",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSecurityGroup",
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Sid" : "ConsoleFullAccess17",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
```

```
    {
      "Sid" : "ConsoleFullAccess18",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess19",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess20",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
```

```
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess21",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume",
        "ec2:StartInstances",
        "ec2:GetConsoleOutput",
        "ec2:GetConsoleScreenshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AWSDRS" : "AllowLaunchingIntoThisInstance"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess22",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
```

```
      "Sid" : "ConsoleFullAccess23",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess24",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess25",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "Bool" : {
```

```
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess26",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateSecurityGroup",
            "CreateVolume",
            "CreateSnapshot",
            "RunInstances"
          ]
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess27",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateLaunchTemplate"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess28",
      "Effect" : "Allow",
```

```
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess29",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess30",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElasticDisasterRecoveryConsoleFullAccess_v2

Keterangan: Kebijakan ini menyediakan akses penuh ke semua publik APIs AWS Elastic Disaster Recovery (AWS DRS), serta semua publik APIs di AWS layanan lain yang digunakan oleh AWS DRS Console. Lampirkan kebijakan ini ke pengguna atau peran Anda.

`AWSElasticDisasterRecoveryConsoleFullAccess_v2`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticDisasterRecoveryConsoleFullAccess_v2` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 November 2023, 13:35 UTC
- Waktu yang telah diedit: 02 Juli 2025, 15:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryConsoleFullAccess_v2`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ConsoleFullAccess1",
      "Effect" : "Allow",
      "Action" : [
        "drs:*"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess2",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetEbsDefaultKmsKeyId",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeHosts",
        "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"
        }
```

```
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElasticDisasterRecoveryConversionServerPolicy

Deskripsi: Kebijakan ini dilampirkan pada peran instans server AWS Elastic Disaster Recovery Conversion. Kebijakan ini memungkinkan Server Konversi Elastic Disaster Recovery (DRS), yang merupakan EC2 instans yang diluncurkan oleh Elastic Disaster Recovery, untuk berkomunikasi dengan layanan DRS. Peran IAM dengan kebijakan ini dilampirkan (sebagai Profil EC2 Instance) oleh DRS ke Server Konversi DRS, yang secara otomatis diluncurkan dan dihentikan oleh DRS, bila diperlukan. Kami tidak menyarankan Anda melampirkan kebijakan ini ke pengguna atau peran IAM Anda. DRS Conversion Server digunakan oleh Elastic Disaster Recovery ketika pengguna memilih untuk memulihkan server sumber menggunakan konsol DRS, CLI, atau API.

`AWSElasticDisasterRecoveryConversionServerPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticDisasterRecoveryConversionServerPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 17 November 2021 13:42 UTC
- Waktu telah diedit: 27 November 2023, 13:13 UTC

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

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSConversionServerPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:SendClientMetricsForDrs",
        "drs:SendClientLogsForDrs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSConversionServerPolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:GetChannelCommandsForDrs",
        "drs:SendChannelCommandResultForDrs"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElasticDisasterRecoveryCrossAccountReplicationPolicy

Deskripsi: Kebijakan ini memungkinkan AWS Elastic Disaster Recovery (DRS) untuk mendukung replikasi lintas akun dan kegagalan lintas akun.

`AWSElasticDisasterRecoveryCrossAccountReplicationPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticDisasterRecoveryCrossAccountReplicationPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 14 Mei 2023, 07:16 UTC
- Waktu telah diedit: 17 Januari 2024, 13:19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryCrossAccountReplicationPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
    {
      "Sid" : "CrossAccountPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumeAttribute",
        "ec2:DescribeInstances",
        "drs:DescribeSourceServers",
        "drs:DescribeReplicationConfigurationTemplates",
        "drs:CreateSourceServerForDrs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CrossAccountPolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:TagResource"
      ],
      "Resource" : "arn:aws:drs:*:*:source-server/*",
      "Condition" : {
        "StringEquals" : {
          "drs:CreateAction" : "CreateSourceServerForDrs"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElasticDisasterRecoveryEc2InstancePolicy

Deskripsi: Kebijakan ini memungkinkan penginstalan dan penggunaan Agen AWS Replikasi, yang digunakan oleh AWS Elastic Disaster Recovery (DRS) untuk memulihkan server sumber yang

berjalan EC2 (lintas wilayah atau lintas AZ). Peran IAM dengan kebijakan ini harus dilampirkan (sebagai Profil EC2 Instance) ke EC2 Instans.

`AWSElasticDisasterRecoveryEc2InstancePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticDisasterRecoveryEc2InstancePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 26 Mei 2022, 12:30 UTC
- Waktu telah diedit: 27 November 2023, 13:39 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryEc2InstancePolicy`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSEc2InstancePolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:GetAgentInstallationAssetsForDrs",
        "drs:SendClientLogsForDrs",
        "drs:SendClientMetricsForDrs",
        "drs:CreateSourceServerForDrs",
        "drs:CreateSourceNetwork"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSEc2InstancePolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:TagResource"
      ],
      "Resource" : "arn:aws:drs:*:*:source-server/*",
      "Condition" : {
        "StringEquals" : {
          "drs:CreateAction" : "CreateSourceServerForDrs"
        }
      }
    },
    {
      "Sid" : "DRSEc2InstancePolicy3",
      "Effect" : "Allow",
      "Action" : [
        "drs:TagResource"
      ],
      "Resource" : "arn:aws:drs:*:*:source-network/*",
      "Condition" : {
        "StringEquals" : {
          "drs:CreateAction" : "CreateSourceNetwork"
        }
      }
    },
    {
      "Sid" : "DRSEc2InstancePolicy4",
      "Effect" : "Allow",
      "Action" : [
        "drs:SendAgentMetricsForDrs",
        "drs:SendAgentLogsForDrs",
        "drs:UpdateAgentSourcePropertiesForDrs",
        "drs:UpdateAgentReplicationInfoForDrs",
        "drs:UpdateAgentConversionInfoForDrs",
        "drs:GetAgentCommandForDrs",
        "drs:GetAgentConfirmedResumeInfoForDrs",
        "drs:GetAgentRuntimeConfigurationForDrs",
        "drs:UpdateAgentBacklogForDrs",
        "drs:GetAgentReplicationInfoForDrs"
      ],
```

```
      "Resource" : "arn:aws:drs:*:*:source-server/*"
    },
    {
      "Sid" : "DRSEc2InstancePolicy5",
      "Effect" : "Allow",
      "Action" : [
        "sts:AssumeRole",
        "sts:TagSession"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/DRSCrossAccountAgentAuthorizedRole_*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/SourceInstanceARN" : "${ec2:SourceInstanceARN}"
        },
        "ForAnyValue:StringEquals" : {
          "sts:TransitiveTagKeys" : "SourceInstanceARN"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElasticDisasterRecoveryFailbackInstallationPolicy

Deskripsi: Anda dapat melampirkan AWSElastic DisasterRecoveryFailbackInstallationPolicy kebijakan ke identitas IAM Anda. Kebijakan ini memungkinkan penginstalan Elastic Disaster Recovery Failback Client, yang digunakan untuk mengembalikan Instans Pemulihan kembali ke infrastruktur sumber asli Anda. Lampirkan kebijakan ini ke pengguna IAM atau peran yang kredensialnya Anda berikan saat menjalankan Klien Kegagalan Pemulihan Bencana Elastis.

`AWSElasticDisasterRecoveryFailbackInstallationPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticDisasterRecoveryFailbackInstallationPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 17 November 2021, 11:02 UTC
- Waktu telah diedit: 27 November 2023, 13:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryFailbackInstallationPolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSFailbackInstallationPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:SendClientLogsForDrs",
        "drs:SendClientMetricsForDrs",
        "drs:DescribeRecoveryInstances",
        "drs:DescribeSourceServers"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "DRSFailbackInstallationPolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:TagResource",
        "drs:IssueAgentCertificateForDrs",
        "drs:AssociateFailbackClientToRecoveryInstanceForDrs",
        "drs:GetSuggestedFailbackClientDeviceMappingForDrs",
        "drs:UpdateAgentReplicationInfoForDrs",
        "drs:UpdateFailbackClientDeviceMappingForDrs"
      ],
      "Resource" : "arn:aws:drs:*:*:recovery-instance/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElasticDisasterRecoveryFailbackPolicy

Deskripsi: Kebijakan ini memungkinkan penggunaan Klien Kegagalan Pemulihan Bencana Elastis, yang digunakan untuk mengembalikan Instans Pemulihan kembali ke infrastruktur sumber asli Anda. Kami tidak menyarankan Anda melampirkan kebijakan ini ke pengguna atau peran IAM Anda.

`AWSElasticDisasterRecoveryFailbackPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticDisasterRecoveryFailbackPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan

- Waktu pembuatan: 17 November 2021 10:41 UTC
- Waktu telah diedit: 27 November 2023, 12:56 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryFailbackPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSFailbackPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:SendClientMetricsForDrs",
        "drs:SendClientLogsForDrs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSFailbackPolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:GetChannelCommandsForDrs",
        "drs:SendChannelCommandResultForDrs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSFailbackPolicy3",
      "Effect" : "Allow",
      "Action" : [
```

```
        "drs:DescribeReplicationServerAssociationsForDrs",
        "drs:DescribeRecoveryInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSFailbackPolicy4",
      "Effect" : "Allow",
      "Action" : [
        "drs:GetFailbackCommandForDrs",
        "drs:UpdateFailbackClientLastSeenForDrs",
        "drs:NotifyAgentAuthenticationForDrs",
        "drs:UpdateAgentReplicationProcessStateForDrs",
        "drs:NotifyAgentReplicationProgressForDrs",
        "drs:NotifyAgentConnectedForDrs",
        "drs:NotifyAgentDisconnectedForDrs",
        "drs:NotifyConsistencyAttainedForDrs",
        "drs:GetFailbackLaunchRequestedForDrs",
        "drs:IssueAgentCertificateForDrs"
      ],
      "Resource" : "arn:aws:drs:*:*:recovery-instance/${aws:SourceIdentity}"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElasticDisasterRecoveryLaunchActionsPolicy

Deskripsi: Kebijakan ini memungkinkan Anda untuk menggunakan Amazon SSM dan layanan tambahan izin yang diperlukan untuk menjalankan tindakan pasca-peluncuran di AWS Elastic Disaster Recovery (AWS DRS). Lampirkan kebijakan ini ke peran atau pengguna IAM Anda.

`AWSElasticDisasterRecoveryLaunchActionsPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticDisasterRecoveryLaunchActionsPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 13 September 2023, 07:38 UTC
- Waktu yang telah diedit: 02 Juli 2025, 15:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryLaunchActionsPolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElasticDisasterRecoveryNetworkReplicationPolicy

Deskripsi: Kebijakan ini memungkinkan AWS Elastic Disaster Recovery (DRS) untuk mendukung replikasi jaringan.

`AWSElasticDisasterRecoveryNetworkReplicationPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticDisasterRecoveryNetworkReplicationPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 11 Juni 2023, 12:36 UTC
- Waktu telah diedit: 02 Januari 2024, 13:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryNetworkReplicationPolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSNetworkReplicationPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeDhcpOptions",
```

```
        "ec2:DescribeInstances",
        "ec2:DescribeManagedPrefixLists",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetManagedPrefixListAssociations"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElasticDisasterRecoveryReadOnlyAccess

Deskripsi: Anda dapat melampirkan AWSElastic DisasterRecoveryReadOnlyAccess kebijakan ke identitas IAM Anda. Kebijakan ini memberikan izin kepada semua publik APIs read-only Elastic Disaster Recovery (DRS), serta beberapa AWS layanan read-only APIs lainnya yang diperlukan untuk menggunakan konsol DRS hanya baca secara penuh. Lampirkan kebijakan ini ke pengguna atau peran IAM Anda.

`AWSElasticDisasterRecoveryReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticDisasterRecoveryReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 17 November 2021 10:50 UTC
- Waktu telah diedit: 29 Juli 2024, 19:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSReadOnlyAccess1",
      "Effect" : "Allow",
      "Action" : [
        "drs:DescribeJobLogItems",
        "drs:DescribeJobs",
        "drs:DescribeRecoveryInstances",
        "drs:DescribeRecoverySnapshots",
        "drs:DescribeReplicationConfigurationTemplates",
        "drs:DescribeSourceServers",
        "drs:GetFailbackReplicationConfiguration",
        "drs:GetLaunchConfiguration",
        "drs:GetReplicationConfiguration",
        "drs:ListExtensibleSourceServers",
        "drs:ListStagingAccounts",
        "drs:ListTagsForResource",
        "drs:ListLaunchActions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSReadOnlyAccess2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "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"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElasticDisasterRecoveryRecoveryInstancePolicy

Deskripsi: Kebijakan ini dilampirkan pada peran instans pemulihan Elastic Disaster Recovery. Kebijakan ini memungkinkan Elastic Disaster Recovery (DRS) Recovery Instance, yang merupakan EC2 instans yang diluncurkan oleh Elastic Disaster Recovery - untuk berkomunikasi dengan layanan DRS, dan untuk dapat gagal kembali ke infrastruktur sumber aslinya. Peran IAM dengan kebijakan ini dilampirkan (sebagai Profil EC2 Instance) oleh Elastic Disaster Recovery ke Instans Pemulihan DRS. Kami tidak menyarankan Anda melampirkan kebijakan ini ke pengguna atau peran IAM Anda.

`AWSElasticDisasterRecoveryRecoveryInstancePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticDisasterRecoveryRecoveryInstancePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan

- Waktu pembuatan: 17 November 2021 10:20 UTC
- Waktu telah diedit: 27 November 2023, 13:11 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryRecoveryInstancePolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSRecoveryInstancePolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:SendAgentMetricsForDrs",
        "drs:SendAgentLogsForDrs",
        "drs:UpdateAgentSourcePropertiesForDrs",
        "drs:UpdateAgentReplicationInfoForDrs",
        "drs:UpdateAgentConversionInfoForDrs",
        "drs:GetAgentCommandForDrs",
        "drs:GetAgentConfirmedResumeInfoForDrs",
        "drs:GetAgentRuntimeConfigurationForDrs",
        "drs:UpdateAgentBacklogForDrs",
        "drs:GetAgentReplicationInfoForDrs",
        "drs:UpdateReplicationCertificateForDrs",
        "drs:NotifyReplicationServerAuthenticationForDrs"
      ],
      "Resource" : "arn:aws:drs:*:*:recovery-instance/*",
      "Condition" : {
        "StringEquals" : {
          "drs:EC2InstanceARN" : "${ec2:SourceInstanceARN}"
        }
      }
```

```
    },
    {
      "Sid" : "DRSRecoveryInstancePolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:DescribeRecoveryInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSRecoveryInstancePolicy3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceTypes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSRecoveryInstancePolicy4",
      "Effect" : "Allow",
      "Action" : [
        "drs:GetAgentInstallationAssetsForDrs",
        "drs:SendClientLogsForDrs",
        "drs:CreateSourceServerForDrs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSRecoveryInstancePolicy5",
      "Effect" : "Allow",
      "Action" : [
        "drs:TagResource"
      ],
      "Resource" : "arn:aws:drs:*:*:source-server/*",
      "Condition" : {
        "StringEquals" : {
          "drs:CreateAction" : "CreateSourceServerForDrs"
        }
      }
    },
    {
      "Sid" : "DRSRecoveryInstancePolicy6",
      "Effect" : "Allow",
      "Action" : [
```

```
        "drs:SendAgentMetricsForDrs",
        "drs:SendAgentLogsForDrs",
        "drs:UpdateAgentSourcePropertiesForDrs",
        "drs:UpdateAgentReplicationInfoForDrs",
        "drs:UpdateAgentConversionInfoForDrs",
        "drs:GetAgentCommandForDrs",
        "drs:GetAgentConfirmedResumeInfoForDrs",
        "drs:GetAgentRuntimeConfigurationForDrs",
        "drs:UpdateAgentBacklogForDrs",
        "drs:GetAgentReplicationInfoForDrs"
      ],
      "Resource" : "arn:aws: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"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElasticDisasterRecoveryReplicationServerPolicy

Deskripsi: Kebijakan ini dilampirkan pada peran instans server Elastic Disaster Recovery Replication. Kebijakan ini memungkinkan Server Replikasi Elastic Disaster Recovery (DRS), yang merupakan EC2 instans yang diluncurkan oleh Elastic Disaster Recovery - untuk berkomunikasi dengan layanan DRS, dan membuat snapshot EBS di situs Anda. Akun AWS Peran IAM dengan kebijakan ini dilampirkan (sebagai Profil EC2 Instance) oleh Elastic Disaster Recovery ke Server Replikasi DRS yang secara otomatis diluncurkan dan dihentikan oleh DRS, sesuai kebutuhan. Server Replikasi DRS digunakan untuk memfasilitasi replikasi data dari server eksternal Anda ke AWS, sebagai bagian dari proses pemulihan yang dikelola oleh DRS. Kami tidak menyarankan Anda melampirkan kebijakan ini ke pengguna atau peran IAM Anda.

`AWSElasticDisasterRecoveryReplicationServerPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticDisasterRecoveryReplicationServerPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 17 November 2021 13:34 UTC
- Waktu telah diedit: 27 November 2023, 13:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryReplicationServerPolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSReplicationServerPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:SendClientMetricsForDrs",
        "drs:SendClientLogsForDrs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSReplicationServerPolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:GetChannelCommandsForDrs",
        "drs:SendChannelCommandResultForDrs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSReplicationServerPolicy3",
      "Effect" : "Allow",
      "Action" : [
        "drs:GetAgentSnapshotCreditsForDrs",
        "drs:DescribeReplicationServerAssociationsForDrs",
        "drs:DescribeSnapshotRequestsForDrs",
        "drs:BatchDeleteSnapshotRequestForDrs",
        "drs:NotifyAgentAuthenticationForDrs",
        "drs:BatchCreateVolumeSnapshotGroupForDrs",
        "drs:UpdateAgentReplicationProcessStateForDrs",
        "drs:NotifyAgentReplicationProgressForDrs",
        "drs:NotifyAgentConnectedForDrs",
        "drs:NotifyAgentDisconnectedForDrs",
        "drs:NotifyVolumeEventForDrs",
        "drs:SendVolumeStatsForDrs"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "DRSReplicationServerPolicy4",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSReplicationServerPolicy5",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSReplicationServerPolicy6",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSReplicationServerPolicy7",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateSnapshot"
        }
      }
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElasticDisasterRecoveryServiceRolePolicy

Deskripsi: Kebijakan ini memungkinkan Elastic Disaster Recovery untuk mengelola AWS sumber daya atas nama Anda.

`AWSElasticDisasterRecoveryServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 17 November 2021 10:56 UTC
- Waktu telah diedit: 05 Januari 2025, 14:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticDisasterRecoveryServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSServiceRolePolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSServiceRolePolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:TagResource"
      ],
      "Resource" : "arn:aws:drs:*:*:recovery-instance/*"
    },
    {
      "Sid" : "DRSServiceRolePolicy3",
      "Effect" : "Allow",
      "Action" : [
        "drs:CreateRecoveryInstanceForDrs",
        "drs:TagResource"
      ],
      "Resource" : "arn:aws:drs:*:*:source-server/*"
    },
    {
      "Sid" : "DRSServiceRolePolicy4",
      "Effect" : "Allow",
      "Action" : "iam:GetInstanceProfile",
      "Resource" : "*"
    },
    {
      "Sid" : "DRSServiceRolePolicy5",
      "Effect" : "Allow",
```

```
      "Action" : "kms:ListRetirableGrants",
      "Resource" : "*"
    },
    {
      "Sid" : "DRSServiceRolePolicy6",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumeAttribute",
        "ec2:GetEbsDefaultKmsKeyId",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeRouteTables",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeManagedPrefixLists",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetManagedPrefixListAssociations",
        "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/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElasticDisasterRecoveryStagingAccountPolicy

Deskripsi: Kebijakan ini memungkinkan akses hanya-baca ke sumber daya AWS Elastic Disaster Recovery (DRS) seperti server sumber dan pekerjaan. Ini juga memungkinkan membuat snapshot yang dikonversi dan berbagi snapshot EBS itu dengan akun tertentu.

`AWSElasticDisasterRecoveryStagingAccountPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticDisasterRecoveryStagingAccountPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 26 Mei 2022, 09:49 UTC
- Waktu telah diedit: 27 November 2023, 13:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryStagingAccountPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSStagingAccountPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:DescribeSourceServers",
        "drs:DescribeRecoverySnapshots",
        "drs:CreateConvertedSnapshotForDrs",
        "drs:GetReplicationConfiguration",
        "drs:DescribeJobs",
        "drs:DescribeJobLogItems"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSStagingAccountPolicy2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:Add/userId" : "${aws:SourceIdentity}"
        },
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElasticDisasterRecoveryStagingAccountPolicy_v2

Deskripsi: Kebijakan ini digunakan oleh AWS Elastic Disaster Recovery (DRS) untuk memulihkan server sumber ke akun target terpisah dan untuk memungkinkan kegagalan kembali. Kami tidak menyarankan Anda melampirkan kebijakan ini ke pengguna atau peran IAM Anda.

`AWSElasticDisasterRecoveryStagingAccountPolicy_v2`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticDisasterRecoveryStagingAccountPolicy_v2` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 05 Januari 2023, 12:11 UTC
- Waktu telah diedit: November 27, 2023, 13:32 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryStagingAccountPolicy_v2`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSStagingAccountPolicyv21",
      "Effect" : "Allow",
      "Action" : [
```

```
        "drs:DescribeSourceServers",
        "drs:DescribeRecoverySnapshots",
        "drs:CreateConvertedSnapshotForDrs",
        "drs:GetReplicationConfiguration",
        "drs:DescribeJobs",
        "drs:DescribeJobLogItems"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSStagingAccountPolicyv22",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:Add/userId" : "${aws:SourceIdentity}"
        },
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSStagingAccountPolicyv23",
      "Effect" : "Allow",
      "Action" : "drs:IssueAgentCertificateForDrs",
      "Resource" : [
        "arn:aws:drs:*:*:source-server/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElasticLoadBalancingClassicServiceRolePolicy

Deskripsi: Kebijakan Peran Tertaut Layanan untuk Bidang Kontrol AWS Elastic Load Balancing - Klasik

`AWSElasticLoadBalancingClassicServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 19 September 2017, 22:36 UTC
- Waktu yang telah diedit: 07 Oktober 2019, 23:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticLoadBalancingClassicServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAddresses",
        "ec2:DescribeInstances",
```

```
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeVpcClassicLink",
        "ec2:CreateSecurityGroup",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:AttachNetworkInterface",
        "ec2:DetachNetworkInterface",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssignIpv6Addresses",
        "ec2:UnassignIpv6Addresses"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElasticLoadBalancingServiceRolePolicy

Deskripsi: Kebijakan Peran Tertaut Layanan untuk Bidang AWS Kontrol Elastic Load Balancing

`AWSElasticLoadBalancingServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 19 September 2017, 22:19 UTC
- Waktu telah diedit: 17 Februari 2025, 20:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticLoadBalancingServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAddresses",
        "ec2:DescribeCoipPools",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeVpcClassicLink",
        "ec2:CreateSecurityGroup",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:GetCoipPoolUsage",
```

```
        "ec2: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:AllocateIpamPoolCidr",
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries",
        "outposts:GetOutpostInstanceTypes"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElementalMediaConnectFullAccess

Deskripsi: Menyediakan akses penuh ke MediaConnect sumber daya AWS Elemental.

`AWSElementalMediaConnectFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElementalMediaConnectFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 12 Februari 2025, 20:07 UTC
- Waktu yang telah diedit: 12 Februari 2025, 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConnectFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElementalMediaConnectReadOnlyAccess

Deskripsi: Menyediakan akses hanya-baca ke sumber daya AWS Elemental MediaConnect .

`AWSElementalMediaConnectReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElementalMediaConnectReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 12 Februari 2025, 20:07 UTC
- Waktu telah diedit: 12 Februari 2025, 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConnectReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElementalMediaConvertFullAccess

Deskripsi: Menyediakan akses penuh ke AWS Elemental MediaConvert melalui AWS Management Console dan SDK.

`AWSElementalMediaConvertFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElementalMediaConvertFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 25 Juni 2018, 19:25 UTC

- Waktu yang telah diedit: 10 Juni 2019, 22:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConvertFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mediaconvert:*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "mediaconvert.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElementalMediaConvertReadOnly

Deskripsi: Menyediakan akses baca saja ke AWS Elemental MediaConvert melalui AWS Management Console dan SDK.

`AWSElementalMediaConvertReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElementalMediaConvertReadOnly` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 25 Juni 2018, 19:25 UTC
- Waktu yang telah diedit: 10 Juni 2019, 22:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConvertReadOnly`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mediaconvert:Get*",
        "mediaconvert:List*",
        "mediaconvert:DescribeEndpoints",
        "s3:ListAllMyBuckets",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElementalMediaLiveFullAccess

Deskripsi: Menyediakan akses penuh ke sumber daya AWS Elemental MediaLive

`AWSElementalMediaLiveFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElementalMediaLiveFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 08 Juli 2020, 17:07 UTC
- Waktu yang telah diedit: 08 Juli 2020, 17:07 UTC

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

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElementalMediaLiveReadOnly

Deskripsi: Menyediakan akses baca saja ke sumber daya AWS Elemental MediaLive

`AWSElementalMediaLiveReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElementalMediaLiveReadOnly` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 08 Juli 2020, 16:38 UTC
- Waktu yang telah diedit: 22 Juli 2024, 17:08 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaLiveReadOnly`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElementalMediaPackageFullAccess

Deskripsi: Menyediakan akses penuh ke sumber daya AWS Elemental MediaPackage

`AWSElementalMediaPackageFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElementalMediaPackageFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 Desember 2017, 23:39 UTC
- Waktu telah diedit: 29 Desember 2017, 23:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElementalMediaPackageReadOnly

Deskripsi: Menyediakan akses baca saja ke sumber daya AWS Elemental MediaPackage

`AWSElementalMediaPackageReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElementalMediaPackageReadOnly` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 Desember 2017, 00:04 UTC
- Waktu diedit: 30 Desember 2017, 00:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageReadOnly`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "mediapackage:List*",
      "mediapackage:Describe*"
    ],
    "Resource" : "*"
  }
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElementalMediaPackageV2FullAccess

Deskripsi: Menyediakan akses penuh ke sumber daya AWS Elemental MediaPackage V2.

`AWSElementalMediaPackageV2FullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElementalMediaPackageV2FullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 25 Juli 2023, 20:29 UTC
- Waktu yang telah diedit: 25 Juli 2023, 20:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageV2FullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : "mediapackagev2:*",
    "Resource" : "*"
  }
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElementalMediaPackageV2ReadOnly

Deskripsi: Menyediakan akses hanya-baca ke sumber daya AWS Elemental V2 MediaPackage.

`AWSElementalMediaPackageV2ReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElementalMediaPackageV2ReadOnly` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 25 Juli 2023, 20:31 UTC

- Waktu yang telah diedit: 25 Juli 2023, 20:31 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageV2ReadOnly`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "mediapackagev2:List*",
      "mediapackagev2:Get*"
    ],
    "Resource" : "*"
  }
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElementalMediaStoreFullAccess

Deskripsi: Menyediakan akses baca dan tulis lengkap ke semua MediaStore APIs

`AWSElementalMediaStoreFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElementalMediaStoreFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 05 Maret 2018, 23:15 UTC
- Waktu telah diedit: 05 Maret 2018, 23:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaStoreFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mediastore:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:SecureTransport" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElementalMediaStoreReadOnly

Deskripsi: Menyediakan izin baca-saja untuk MediaStore APIs

`AWSElementalMediaStoreReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElementalMediaStoreReadOnly` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 08 Maret 2018, 19:48 UTC
- Waktu telah diedit: 08 Maret 2018, 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaStoreReadOnly`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mediastore:Get*",
        "mediastore:List*",
        "mediastore:Describe*"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:SecureTransport" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElementalMediaTailorFullAccess

Deskripsi: Menyediakan akses penuh ke sumber daya AWS Elemental MediaTailor

`AWSElementalMediaTailorFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElementalMediaTailorFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 23 November 2021, 00:04 UTC
- Waktu yang telah diedit: 23 November 2021, 00:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaTailorFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElementalMediaTailorReadOnly

Deskripsi: Menyediakan akses baca saja ke sumber daya AWS Elemental MediaTailor

`AWSElementalMediaTailorReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElementalMediaTailorReadOnly` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 23 November 2021, 00:05 UTC
- Waktu yang telah diedit: 23 November 2021, 00:05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaTailorReadOnly`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSEnhancedClassicNetworkingMangementPolicy

Deskripsi: Kebijakan untuk mengaktifkan fitur manajemen jaringan klasik yang disempurnakan.

`AWSEnhancedClassicNetworkingMangementPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 20 September 2017, 17:29 UTC
- Waktu yang telah diedit: 20 September 2017, 17:29 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEnhancedClassicNetworkingMangementPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
  "Statement" : [
    {
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSEntityResolutionConsoleFullAccess

Deskripsi: Menyediakan konsol akses penuh ke Resolusi AWS Entitas dan layanan terkait.

`AWSEntityResolutionConsoleFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSEntityResolutionConsoleFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 17 Agustus 2023, 17:54 UTC
- Waktu yang telah diedit: 16 Oktober 2023, 18:46 UTC
- ARN: `arn:aws:iam::aws:policy/AWSEntityResolutionConsoleFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EntityResolutionAccess",
      "Effect" : "Allow",
      "Action" : [
        "entityresolution:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueSourcesConsoleDisplay",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetSchema",
        "glue:SearchTables",
        "glue:GetSchemaByDefinition",
        "glue:GetSchemaVersion",
        "glue:GetSchemaVersionsDiff",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetTableVersion",
        "glue:GetTableVersions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3BucketsConsoleDisplay",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "S3SourcesConsoleDisplay",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:ListBucketVersions",
        "s3:GetBucketVersioning"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TaggingConsoleDisplay",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetTagKeys",
        "tag:GetTagValues"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSConsoleDisplay",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListRolesToPickRoleForPassing",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassRoleToEntityResolutionService",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*entityresolution*",
```

```
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "entityresolution.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ManageEventBridgeRules",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:PutTargets",
        "events:PutRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/entity-resolution-automatic*"
      ]
    },
    {
      "Sid" : "ADXReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:GetDataSet"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSEntityResolutionConsoleReadOnlyAccess

Deskripsi: Menyediakan akses hanya-baca ke Resolusi AWS Entitas melalui. AWS Management Console

`AWSEntityResolutionConsoleReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSEntityResolutionConsoleReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 17 Agustus 2023, 18:18 UTC
- Waktu yang telah diedit: 17 Agustus 2023, 18:18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSEntityResolutionConsoleReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EntityResolutionRead",
      "Effect" : "Allow",
      "Action" : [
        "entityresolution:Get*",
        "entityresolution:List*"
```

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSFaultInjectionSimulatorEC2Access

Deskripsi: Kebijakan ini memberikan izin Layanan Simulator Injeksi Kesalahan di EC2 dan layanan lain yang diperlukan untuk melakukan tindakan FIS.

`AWSFaultInjectionSimulatorEC2Access`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSFaultInjectionSimulatorEC2Access` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 26 Oktober 2022, 20:39 UTC
- Waktu telah diedit: 12 Februari 2025, 10:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorEC2Access`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowEc2Actions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RebootInstances",
        "ec2:SendSpotInstanceInterruptions",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Sid" : "AllowEc2InstancesWithEncryptedEbsVolumes",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : [
        "arn:aws:kms:*:*:key/*"
      ],
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com"
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        }
      }
    },
    {
      "Sid" : "AllowSSMSendOnEc2",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:document/*"
      ]
    },
    {
      "Sid" : "AllowSSMStopOnEc2",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CancelCommand",
        "ssm:ListCommands"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeInstances",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeInstances",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSFaultInjectionSimulatorECSAccess

Deskripsi: Kebijakan ini memberikan izin Layanan Simulator Injeksi Kesalahan di ECS dan layanan lain yang diperlukan untuk melakukan tindakan FIS.

`AWSFaultInjectionSimulatorECSAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSFaultInjectionSimulatorECSAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 26 Oktober 2022, 20:37 UTC
- Waktu telah diedit: 07 Maret 2025, 14:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorECSAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Clusters",
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeClusters",
        "ecs:ListContainerInstances"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:cluster/*"
      ]
    },
    {
      "Sid" : "Tasks",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ecs:DescribeTasks",
        "ecs:StopTask"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:task/*/*"
      ]
    },
    {
      "Sid" : "ContainerInstances",
      "Effect" : "Allow",
      "Action" : [
        "ecs:UpdateContainerInstancesState"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:container-instance/*/*"
      ]
    },
    {
      "Sid" : "ListTasks",
      "Effect" : "Allow",
      "Action" : [
        "ecs:ListTasks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMSend",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*:*:document/*"
      ]
    },
    {
      "Sid" : "SSMList",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListCommands",
        "ssm:CancelCommand"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "TargetResolutionByTags",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSFaultInjectionSimulatorEKSAccess

Deskripsi: Kebijakan ini memberikan izin Layanan Simulator Injeksi Kesalahan di EKS dan layanan lain yang diperlukan untuk melakukan tindakan FIS.

`AWSFaultInjectionSimulatorEKSAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSFaultInjectionSimulatorEKSAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 26 Oktober 2022, 20:34 UTC
- Waktu yang telah diedit: 11 Maret 2025, 14:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorEKSAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeInstances",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeInstances",
      "Resource" : "*"
    },
    {
      "Sid" : "TerminateInstances",
      "Effect" : "Allow",
      "Action" : "ec2:TerminateInstances",
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Sid" : "DescribeSubnets",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeSubnets",
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeCluster",
      "Effect" : "Allow",
      "Action" : "eks:DescribeCluster",
      "Resource" : "arn:aws:eks:*:*:cluster/*"
    },
    {
      "Sid" : "DescribeNodeGroup",
      "Effect" : "Allow",
      "Action" : "eks:DescribeNodegroup",
      "Resource" : "arn:aws:eks:*:*:nodegroup/*"
    },
```

```
    {
      "Sid" : "TargetResolutionByTags",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSFaultInjectionSimulatorNetworkAccess

Deskripsi: Kebijakan ini memberikan izin Layanan Simulator Injeksi Kesalahan dalam EC2 jaringan dan layanan lain yang diperlukan untuk melakukan tindakan FIS.

`AWSFaultInjectionSimulatorNetworkAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSFaultInjectionSimulatorNetworkAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 26 Oktober 2022, 20:32 UTC
- Waktu telah diedit: 11 Maret 2025, 13:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorNetworkAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateTagsOnNetworkAcl",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:network-acl/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkAcl",
          "aws:RequestTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "CreateNetworkAcl",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkAcl",
      "Resource" : "arn:aws:ec2:*:*:network-acl/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "DeleteNetworkAcl",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkAclEntry",
        "ec2:DeleteNetworkAcl"
      ],
```

```
      "Resource" : [
        "arn:aws:ec2:*:*:network-acl/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "CreateNetworkAclOnVpc",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkAcl",
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Sid" : "VpcActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeRouteTables",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGateways"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ReplaceNetworkAclAssociation",
      "Effect" : "Allow",
      "Action" : "ec2:ReplaceNetworkAclAssociation",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-acl/*"
      ]
    },
    {
```

```
      "Sid" : "GetManagedPrefixListEntries",
      "Effect" : "Allow",
      "Action" : "ec2:GetManagedPrefixListEntries",
      "Resource" : "arn:aws:ec2:*:*:prefix-list/*"
    },
    {
      "Sid" : "CreateRouteTable",
      "Effect" : "Allow",
      "Action" : "ec2:CreateRouteTable",
      "Resource" : "arn:aws:ec2:*:*:route-table/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "CreateRouteTableOnVpc",
      "Effect" : "Allow",
      "Action" : "ec2:CreateRouteTable",
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Sid" : "CreateTagsOnRouteTable",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:route-table/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateRouteTable",
          "aws:RequestTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTagsOnNetworkInterface",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface",
          "aws:RequestTag/managedByFIS" : "true"
        }
```

```
      }
    },
    {
      "Sid" : "CreateTagsOnPrefixList",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:prefix-list/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateManagedPrefixList",
          "aws:RequestTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "DeleteRouteTable",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteRouteTable",
      "Resource" : [
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "CreateRoute",
      "Effect" : "Allow",
      "Action" : "ec2:CreateRoute",
      "Resource" : "arn:aws:ec2:*:*:route-table/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "CreateNetworkInterface",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "CreateNetworkInterfaceOnSubnet",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "DeleteNetworkInterface",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "CreateManagedPrefixList",
      "Effect" : "Allow",
      "Action" : "ec2:CreateManagedPrefixList",
      "Resource" : "arn:aws:ec2:*:*:prefix-list/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "DeleteManagedPrefixList",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteManagedPrefixList",
      "Resource" : "arn:aws:ec2:*:*:prefix-list/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "ec2:ResourceTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "ModifyManagedPrefixList",
      "Effect" : "Allow",
      "Action" : "ec2:ModifyManagedPrefixList",
      "Resource" : "arn:aws:ec2:*:*:prefix-list/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "ReplaceRouteTableAssociation",
      "Effect" : "Allow",
      "Action" : "ec2:ReplaceRouteTableAssociation",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*"
      ]
    },
    {
      "Sid" : "AssociateRouteTable",
      "Effect" : "Allow",
      "Action" : "ec2:AssociateRouteTable",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*"
      ]
    },
    {
      "Sid" : "DisassociateRouteTable",
      "Effect" : "Allow",
      "Action" : "ec2:DisassociateRouteTable",
      "Resource" : [
        "arn:aws:ec2:*:*:route-table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/managedByFIS" : "true"
        }
```

```
      }
    },
    {
      "Sid" : "DisassociateRouteTableOnSubnet",
      "Effect" : "Allow",
      "Action" : "ec2:DisassociateRouteTable",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Sid" : "ModifyVpcEndpointOnRouteTable",
      "Effect" : "Allow",
      "Action" : "ec2:ModifyVpcEndpoint",
      "Resource" : [
        "arn:aws:ec2:*:*:route-table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "ModifyVpcEndpoint",
      "Effect" : "Allow",
      "Action" : "ec2:ModifyVpcEndpoint",
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ]
    },
    {
      "Sid" : "TransitGatewayRouteTableAssociation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DisassociateTransitGatewayRouteTable",
        "ec2:AssociateTransitGatewayRouteTable"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:transit-gateway-route-table/*",
        "arn:aws:ec2:*:*:transit-gateway-attachment/*"
      ]
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSFaultInjectionSimulatorRDSAccess

Deskripsi: Kebijakan ini memberikan izin Layanan Simulator Injeksi Kesalahan di RDS dan layanan lain yang diperlukan untuk melakukan tindakan FIS.

`AWSFaultInjectionSimulatorRDSAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSFaultInjectionSimulatorRDSAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 26 Oktober 2022, 20:30 UTC
- Waktu telah diedit: 18 Maret 2025, 15:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorRDSAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowFailover",
      "Effect" : "Allow",
      "Action" : [
        "rds:FailoverDBCluster"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "AllowReboot",
      "Effect" : "Allow",
      "Action" : [
        "rds:RebootDBInstance"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:db:*"
      ]
    },
    {
      "Sid" : "DescribeResources",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TargetResolutionByTags",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSFaultInjectionSimulatorSSMAccess

Deskripsi: Kebijakan ini memberikan izin Layanan Simulator Injeksi Kesalahan di SSM dan layanan lain yang diperlukan untuk melakukan tindakan FIS.

`AWSFaultInjectionSimulatorSSMAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSFaultInjectionSimulatorSSMAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 26 Oktober 2022, 15:33 UTC
- Waktu yang telah diedit: 25 Juni 2025, 14:22 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorSSMAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*: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" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSFinSpaceServiceRolePolicy

Deskripsi: Kebijakan untuk mengaktifkan akses ke Layanan AWS dan Sumber Daya yang digunakan atau dikelola oleh Amazon FinSpace

`AWSFinSpaceServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 12 Mei 2023, 16:42 UTC
- Waktu telah diedit: 01 Desember 2023, 21:05 UTC

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

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSFMAdminFullAccess

Deskripsi: Akses penuh untuk Administrator AWS FM

`AWSFMAdminFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSFMAdminFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 09 Mei 2018, 18:06 UTC
- Waktu yang telah diedit: 20 Oktober 2022, 23.39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSFMAdminFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "fms:*",
        "waf:*",
        "waf-regional:*",
        "elasticloadbalancing:SetWebACL",
        "firehose:ListDeliveryStreams",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
```

```
        "organizations:ListRoots",
        "organizations:ListChildren",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListOrganizationalUnitsForParent",
        "shield:GetSubscriptionState",
        "route53resolver:ListFirewallRuleGroups",
        "route53resolver:GetFirewallRuleGroup",
        "wafv2:ListRuleGroups",
        "wafv2:ListAvailableManagedRuleGroups",
        "wafv2:CheckCapacity",
        "wafv2:PutLoggingConfiguration",
        "wafv2:ListAvailableManagedRuleGroupVersions",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:DescribeRuleGroupMetadata",
        "network-firewall:ListRuleGroups",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeRegions"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketPolicy",
        "s3:GetBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-waf-logs-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "fms.amazonaws.com"
          ]
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:ListDelegatedAdministrators",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "fms.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSFMAdminReadOnlyAccess

Deskripsi: Akses hanya baca untuk Administrator AWS FM yang memungkinkan pemantauan operasi AWS FM

`AWSFMAdminReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSFMAdminReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 09 Mei 2018, 20:07 UTC
- Waktu telah diedit: 31 Oktober 2022, 22.42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSFMAdminReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "fms:Get*",
        "fms:List*",
        "waf:Get*",
        "waf:List*",
        "waf-regional:Get*",
        "waf-regional:List*",
        "firehose:ListDeliveryStreams",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "organizations:ListRoots",
        "organizations:ListChildren",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListOrganizationalUnitsForParent",
        "shield:GetSubscriptionState",
        "route53resolver:ListFirewallRuleGroups",
        "route53resolver:GetFirewallRuleGroup",
        "wafv2:ListRuleGroups",
        "wafv2:ListAvailableManagedRuleGroups",
        "wafv2:CheckCapacity",
        "wafv2:ListAvailableManagedRuleGroupVersions",
```

```
        "network-firewall:DescribeRuleGroup",
        "network-firewall:DescribeRuleGroupMetadata",
        "network-firewall:ListRuleGroups",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeRegions"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-waf-logs-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "fms.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSFMMemberReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke tindakan AWS WAF untuk akun anggota AWS Firewall Manager

`AWSFMMemberReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSFMMemberReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 09 Mei 2018, 21:05 UTC
- Waktu yang telah diedit: 09 Mei 2018, 21:05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSFMMemberReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "fms:GetAdminAccount",
        "waf:Get*",
        "waf:List*",
        "waf-regional:Get*",
        "waf-regional:List*",
        "organizations:DescribeOrganization"
      ],
```

```
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSForWordPressPluginPolicy

Deskripsi: Kebijakan yang dikelola untuk AWS Untuk Plugin Wordpress

`AWSForWordPressPluginPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSForWordPressPluginPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 Oktober 2019 00:27 UTC
- Waktu yang telah diedit: 20 Januari 2020, 23:20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSForWordPressPluginPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Permissions1",
      "Effect" : "Allow",
      "Action" : [
        "polly:SynthesizeSpeech",
        "polly:DescribeVoices",
        "translate:TranslateText"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Permissions2",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:CreateBucket",
        "s3:PutObjectAcl"
      ],
      "Resource" : [
        "arn:aws:s3:::audio_for_wordpress*",
        "arn:aws:s3:::audio-for-wordpress*"
      ]
    },
    {
      "Sid" : "Permissions3",
      "Effect" : "Allow",
      "Action" : [
        "acm:AddTagsToCertificate",
        "acm:DescribeCertificate",
        "acm:RequestCertificate",
        "cloudformation:CreateStack",
        "cloudfront:ListDistributions"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "us-east-1"
        }
      }
    },
    {
      "Sid" : "Permissions4",
      "Effect" : "Allow",
      "Action" : [
        "acm:DeleteCertificate",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources",
        "cloudformation:UpdateStack",
        "cloudfront:CreateDistribution",
        "cloudfront:CreateInvalidation",
        "cloudfront:DeleteDistribution",
        "cloudfront:GetDistribution",
        "cloudfront:GetInvalidation",
        "cloudfront:TagResource",
        "cloudfront:UpdateDistribution"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/createdBy" : "AWSForWordPressPlugin"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSGitSyncServiceRolePolicy

Deskripsi: Kebijakan yang memungkinkan Koneksi AWS Kode untuk menyinkronkan konten dari repositori git Anda

`AWSGitSyncServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 16 November 2023, 17:05 UTC
- Waktu yang telah diedit: 26 April 2024, 18:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSGitSyncServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSGlobalAcceleratorSLRPolicy

Deskripsi: Kebijakan yang memberikan izin kepada AWS Global Accelerator untuk mengelola Antarmuka Jaringan EC2 Elastis dan Grup Keamanan.

`AWSGlobalAcceleratorSLRPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 05 April 2019, 19:39 UTC
- Waktu telah diedit: 29 Oktober 2024, 18:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSGlobalAcceleratorSLRPolicy`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2Action1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSubnets",
        "ec2:DescribeRegions",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeAddresses"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2Action2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup",
        "ec2:AssignIpv6Addresses",
        "ec2:UnassignIpv6Addresses"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AWSServiceName" : "GlobalAccelerator"
        }
      }
```

```
    },
    {
      "Sid" : "EC2Action3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "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/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSGlueConsoleFullAccess

Deskripsi: Menyediakan akses penuh ke AWS Glue melalui AWS Management Console

`AWSGlueConsoleFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSGlueConsoleFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 14 Agustus 2017, 13:37 UTC
- Waktu yang telah diedit: 14 Juli 2023, 14:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGlueConsoleFullAccess`

Versi kebijakan

Versi kebijakan: v14 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BaseAppPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:*",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSubnetGroups",
        "iam:ListRoles",
        "iam:ListUsers",
        "iam:ListGroups",
        "iam:ListRolePolicies",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
```

```
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeInstances",
        "ec2:DescribeImages",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "rds:DescribeDBSubnetGroups",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "cloudformation:ListStacks",
        "cloudformation:DescribeStacks",
        "cloudformation:GetTemplateSummary",
        "dynamodb:ListTables",
        "kms:ListAliases",
        "kms:DescribeKey",
        "cloudwatch:GetMetricData",
        "cloudwatch:ListDashboards",
        "databrew:ListRecipes",
        "databrew:ListRecipeVersions",
        "databrew:DescribeRecipe"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*/*",
        "arn:aws:s3:::*/*aws-glue-*/*",
        "arn:aws:s3:::aws-glue-*"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:GetLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:/aws-glue/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/aws-glue*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:image/*",
```

```
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances",
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/aws-glue-*/*"
        },
        "StringEquals" : {
          "ec2:ResourceTag/aws:cloudformation:logical-id" : "ZeppelinInstance"
        }
      }
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/AWSGlueServiceRole*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com"
          ]
        }
      }
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
```

```
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/AWSGlueServiceNotebookRole*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AWSGlueServiceRole*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSGlueConsoleSageMakerNotebookFullAccess

Deskripsi: Menyediakan akses penuh ke AWS Glue melalui AWS Management Console dan akses ke instance notebook sagemaker.

`AWSGlueConsoleSageMakerNotebookFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSGlueConsoleSageMakerNotebookFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 05 Oktober 2018, 17:52 UTC
- Waktu yang telah diedit: 15 Juli 2021 15.24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGlueConsoleSageMakerNotebookFullAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:*",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSubnetGroups",
        "iam:ListRoles",
        "iam:ListRolePolicies",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
```

```
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeInstances",
        "ec2:DescribeImages",
        "ec2:CreateNetworkInterface",
        "ec2:AttachNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeNetworkInterfaces",
        "rds:DescribeDBInstances",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "cloudformation:DescribeStacks",
        "cloudformation:GetTemplateSummary",
        "dynamodb:ListTables",
        "kms:ListAliases",
        "kms:DescribeKey",
        "sagemaker:ListNotebookInstances",
        "cloudformation:ListStacks",
        "cloudwatch:GetMetricData",
        "cloudwatch:ListDashboards"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*/*aws-glue-*/*",
        "arn:aws:s3:::aws-glue-*"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:GetLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:/aws-glue/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/aws-glue*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreatePresignedNotebookInstanceUrl",
        "sagemaker:CreateNotebookInstance",
        "sagemaker:DeleteNotebookInstance",
        "sagemaker:DescribeNotebookInstance",
        "sagemaker:StartNotebookInstance",
        "sagemaker:StopNotebookInstance",
        "sagemaker:UpdateNotebookInstance",
        "sagemaker:ListTags"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:notebook-instance/aws-glue-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeNotebookInstanceLifecycleConfig",
```

```
        "sagemaker:CreateNotebookInstanceLifecycleConfig",
        "sagemaker:DeleteNotebookInstanceLifecycleConfig",
        "sagemaker:ListNotebookInstanceLifecycleConfigs"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:notebook-instance-lifecycle-config/aws-glue-
*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances",
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
 "arn:aws:cloudformation:*:*:stack/aws-glue-*/*"
        },
        "StringEquals" : {
          "ec2:ResourceTag/aws:cloudformation:logical-id" : "ZeppelinInstance"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "aws-glue-*"
          ]
        }
      }
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/AWSGlueServiceRole*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com"
          ]
        }
      }
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/AWSGlueServiceNotebookRole*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Action" : [
```

```
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/AWSGlueServiceSageMakerNotebookRole*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com"
          ]
        }
      }
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AWSGlueServiceRole*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AwsGlueDataBrewFullAccessPolicy

Deskripsi: Menyediakan akses penuh ke AWS Glue DataBrew melalui AWS Management Console. Juga menyediakan akses pilih ke layanan terkait (misalnya, S3, KMS, Glue).

`AwsGlueDataBrewFullAccessPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AwsGlueDataBrewFullAccessPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 11 November 2020, 16:51 UTC
- Waktu yang telah diedit: 04 Februari 2022, 18.28 UTC
- ARN: `arn:aws:iam::aws:policy/AwsGlueDataBrewFullAccessPolicy`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "databrew:CreateDataset",
        "databrew:DescribeDataset",
        "databrew:ListDatasets",
        "databrew:UpdateDataset",
        "databrew:DeleteDataset",
```

```
        "databrew:CreateProject",
        "databrew:DescribeProject",
        "databrew:ListProjects",
        "databrew:StartProjectSession",
        "databrew:SendProjectSessionAction",
        "databrew:UpdateProject",
        "databrew:DeleteProject",
        "databrew:CreateRecipe",
        "databrew:DescribeRecipe",
        "databrew:ListRecipes",
        "databrew:ListRecipeVersions",
        "databrew:PublishRecipe",
        "databrew:UpdateRecipe",
        "databrew:BatchDeleteRecipeVersion",
        "databrew:DeleteRecipeVersion",
        "databrew:CreateRecipeJob",
        "databrew:CreateProfileJob",
        "databrew:DescribeJob",
        "databrew:DescribeJobRun",
        "databrew:ListJobRuns",
        "databrew:ListJobs",
        "databrew:StartJobRun",
        "databrew:StopJobRun",
        "databrew:UpdateProfileJob",
        "databrew:UpdateRecipeJob",
        "databrew:DeleteJob",
        "databrew:CreateSchedule",
        "databrew:DescribeSchedule",
        "databrew:ListSchedules",
        "databrew:UpdateSchedule",
        "databrew:DeleteSchedule",
        "databrew:CreateRuleset",
        "databrew:DeleteRuleset",
        "databrew:DescribeRuleset",
        "databrew:ListRulesets",
        "databrew:UpdateRuleset",
        "databrew:ListTagsForResource",
        "databrew:TagResource",
        "databrew:UntagResource"
      ],
      "Resource" : [
        "*"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "appflow:DescribeFlow",
        "appflow:DescribeFlowExecutionRecords",
        "appflow:ListFlows",
        "glue:GetConnection",
        "glue:GetConnections",
        "glue:GetDatabases",
        "glue:GetPartitions",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetDataCatalogEncryptionSettings",
        "dataexchange:ListDataSets",
        "dataexchange:ListDataSetRevisions",
        "dataexchange:ListRevisionAssets",
        "dataexchange:CreateJob",
        "dataexchange:StartJob",
        "dataexchange:GetJob",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "kms:DescribeKey",
        "kms:ListKeys",
        "kms:ListAliases",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSubnetGroups",
        "redshift-data:DescribeStatement",
        "redshift-data:ListDatabases",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables",
        "s3:ListAllMyBuckets",
        "s3:GetBucketCORS",
        "s3:GetBucketLocation",
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
        "secretsmanager:ListSecrets",
        "secretsmanager:DescribeSecret",
        "sts:GetCallerIdentity",
        "cloudtrail:LookupEvents",
        "iam:ListRoles",
        "iam:GetRole"
      ],
      "Resource" : [
```

```
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateConnection"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:connection/AwsGlueDataBrew-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabases"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateTable"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*/awsgluedatabrew*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::databrew-public-datasets-*"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AwsGlueDataBrew-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateRandom"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:databrew!default-*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "databrew.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:databrew!default-*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:Name" : "databrew!default"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "databrew.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "databrew.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSGlueDataBrewServiceRole

Deskripsi: Kebijakan ini memberikan izin untuk lem untuk melakukan tindakan pada katalog data lem pengguna, kebijakan ini juga memberikan izin untuk tindakan ec2 untuk memungkinkan lem membuat ENI untuk terhubung ke sumber daya di VPC, juga memungkinkan lem untuk mengakses data terdaftar di lakeformation dan izin untuk mengakses cloudwatch pengguna

`AWSGlueDataBrewServiceRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSGlueDataBrewServiceRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 04 Desember 2020, 21:26 UTC
- Waktu telah diedit: 20 Maret 2024, 23:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSGlueDataBrewServiceRole`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GlueDataPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabases",
        "glue:GetPartitions",
        "glue:GetTable",
```

```
        "glue:GetTables",
        "glue:GetConnection"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "GluePIIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:BatchGetCustomEntityTypes",
        "glue:GetCustomEntityType"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "S3PublicDatasetAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::databrew-public-datasets-*"
      ]
    },
    {
      "Sid" : "EC2NetworkingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeRouteTables",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "*"
      ]
```

```
    },
    {
      "Sid" : "EC2DeleteGlueNetworkInterfacePermissions",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteNetworkInterface",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/aws-glue-service-resource" : "*"
        }
      },
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EC2GlueTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws-glue-service-resource"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "GlueDatabrewLogGroupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws-glue-databrew/*"
      ]
```

```
    },
    {
      "Sid" : "LakeFormationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataAccess"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:databrew!default-*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSGlueSchemaRegistryFullAccess

Deskripsi: Menyediakan akses penuh ke Layanan Registri AWS Glue Schema

`AWSGlueSchemaRegistryFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSGlueSchemaRegistryFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 20 November 2020, 00:19 UTC
- Waktu yang telah diedit: 20 November 2020, 00:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGlueSchemaRegistryFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSGlueSchemaRegistryFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateRegistry",
        "glue:UpdateRegistry",
        "glue:DeleteRegistry",
        "glue:GetRegistry",
        "glue:ListRegistries",
        "glue:CreateSchema",
        "glue:UpdateSchema",
        "glue:DeleteSchema",
        "glue:GetSchema",
        "glue:ListSchemas",
        "glue:RegisterSchemaVersion",
        "glue:DeleteSchemaVersions",
        "glue:GetSchemaByDefinition",
        "glue:GetSchemaVersion",
        "glue:GetSchemaVersionsDiff",
        "glue:ListSchemaVersions",
```

```
        "glue:CheckSchemaVersionValidity",
        "glue:PutSchemaVersionMetadata",
        "glue:RemoveSchemaVersionMetadata",
        "glue:QuerySchemaVersionMetadata"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AWSGlueSchemaRegistryTagsFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetTags",
        "glue:TagResource",
        "glue:UnTagResource"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:schema/*",
        "arn:aws:glue:*:*:registry/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSGlueSchemaRegistryReadonlyAccess

Deskripsi: Menyediakan akses readonly ke AWS Glue Schema Registry Service

`AWSGlueSchemaRegistryReadonlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSGlueSchemaRegistryReadonlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 20 November 2020, 00:20 UTC
- Waktu yang telah diedit: 20 November 2020, 00:20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGlueSchemaRegistryReadonlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSGlueSchemaRegistryReadonlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetRegistry",
        "glue:ListRegistries",
        "glue:GetSchema",
        "glue:ListSchemas",
        "glue:GetSchemaByDefinition",
        "glue:GetSchemaVersion",
        "glue:ListSchemaVersions",
        "glue:GetSchemaVersionsDiff",
        "glue:CheckSchemaVersionValidity",
        "glue:QuerySchemaVersionMetadata",
```

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSGlueServiceNotebookRole

Deskripsi: Kebijakan untuk peran layanan AWS Glue yang memungkinkan pelanggan mengelola server notebook

`AWSGlueServiceNotebookRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSGlueServiceNotebookRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 14 Agustus 2017, 13:37 UTC
- Waktu telah diedit: 09 Oktober 2023, 15:59 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSGlueServiceNotebookRole`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:CreatePartition",
        "glue:CreateTable",
        "glue:DeleteDatabase",
        "glue:DeletePartition",
        "glue:DeleteTable",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetTable",
        "glue:GetTableVersions",
        "glue:GetTables",
        "glue:UpdateDatabase",
        "glue:UpdatePartition",
        "glue:UpdateTable",
        "glue:CreateConnection",
        "glue:CreateJob",
        "glue:DeleteConnection",
        "glue:DeleteJob",
        "glue:GetConnection",
        "glue:GetConnections",
        "glue:GetDevEndpoint",
        "glue:GetDevEndpoints",
        "glue:GetJob",
        "glue:GetJobs",
        "glue:UpdateJob",
        "glue:BatchDeleteConnection",
        "glue:UpdateConnection",
        "glue:GetUserDefinedFunction",
        "glue:UpdateUserDefinedFunction",
```

```
        "glue:GetUserDefinedFunctions",
        "glue:DeleteUserDefinedFunction",
        "glue:CreateUserDefinedFunction",
        "glue:BatchGetPartition",
        "glue:BatchDeletePartition",
        "glue:BatchCreatePartition",
        "glue:BatchDeleteTable",
        "glue:UpdateDevEndpoint",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "codewhisperer:GenerateRecommendations"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::crawler-public*",
        "arn:aws:s3:::aws-glue*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:DeleteObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
```

```
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws-glue-service-resource"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSGlueServiceRole

Deskripsi: Kebijakan untuk peran layanan AWS Glue yang memungkinkan akses ke layanan terkait termasuk EC2, S3, dan Cloudwatch Logs

`AWSGlueServiceRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSGlueServiceRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 14 Agustus 2017, 13:37 UTC
- Waktu telah diedit: September 11, 2023, 16:39 UTC

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

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:*",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeRouteTables",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "iam:ListRolePolicies",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "cloudwatch:PutMetricData"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*/*",
        "arn:aws:s3:::*/*aws-glue-*/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::crawler-public*",
        "arn:aws:s3:::aws-glue-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:*:/aws-glue/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
```

```
        "ec2:DeleteTags"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws-glue-service-resource"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AwsGlueSessionUserRestrictedNotebookPolicy

Deskripsi: Menyediakan izin yang memungkinkan pengguna untuk membuat dan menggunakan hanya sesi buku catatan yang terkait dengan pengguna. Kebijakan ini juga mencakup izin untuk secara eksplisit mengizinkan pengguna melewati peran sesi Glue terbatas.

`AwsGlueSessionUserRestrictedNotebookPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AwsGlueSessionUserRestrictedNotebookPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 April 2022, 15:24 UTC
- Waktu yang telah diedit: Agustus 15, 2024, 20:51 UTC
- ARN: `arn:aws:iam::aws:policy/AwsGlueSessionUserRestrictedNotebookPolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "NotebokAllowActions0",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/owner" : "${aws:PrincipalTag/owner}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "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"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AwsGlueSessionUserRestrictedNotebookServiceRole

Deskripsi: Menyediakan akses penuh ke semua sumber daya AWS Glue kecuali untuk sesi. Memungkinkan pengguna untuk membuat dan menggunakan hanya sesi notebook yang terkait dengan pengguna. Kebijakan ini juga mencakup izin lain yang diperlukan oleh AWS Glue untuk mengelola sumber daya Glue di AWS layanan lain.

`AwsGlueSessionUserRestrictedNotebookServiceRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AwsGlueSessionUserRestrictedNotebookServiceRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 18 April 2022, 15:27 UTC
- Waktu yang telah diedit: Agustus 15, 2024, 20:51 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AwsGlueSessionUserRestrictedNotebookServiceRole`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "glue:*",
      "Resource" : [
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:tableVersion/*",
        "arn:aws:glue:*:*:connection/*",
        "arn:aws:glue:*:*:userDefinedFunction/*",
        "arn:aws:glue:*:*:devEndpoint/*",
        "arn:aws:glue:*:*:job/*",
        "arn:aws:glue:*:*:trigger/*",
        "arn:aws:glue:*:*:crawler/*",
        "arn:aws:glue:*:*:workflow/*",
        "arn:aws:glue:*:*:mlTransform/*",
        "arn:aws:glue:*:*:registry/*",
        "arn:aws:glue:*:*:schema/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:RequestTag/owner" : "${aws:PrincipalTag/owner}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
    {
      "Sid" : "AllowGlueTaggingAction",
      "Effect" : "Allow",
      "Action" : [
        "glue:TagResource"
      ],
      "Resource" : "arn:aws:glue:*:*:session/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/owner" : "${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/*"
      ]
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AwsGlueSessionUserRestrictedPolicy

Deskripsi: Menyediakan izin yang memungkinkan pengguna untuk membuat dan menggunakan hanya sesi interaktif yang terkait dengan pengguna. Kebijakan ini juga mencakup izin untuk secara eksplisit mengizinkan pengguna melewati peran sesi Glue terbatas.

`AwsGlueSessionUserRestrictedPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AwsGlueSessionUserRestrictedPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 14 April 2022, 21:31 UTC
- Waktu telah diedit: Agustus 05, 2024, 23:06 UTC
- ARN: `arn:aws:iam::aws:policy/AwsGlueSessionUserRestrictedPolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AwsGlueSessionUserRestrictedServiceRole

Deskripsi: Menyediakan akses penuh ke semua sumber daya AWS Glue kecuali untuk sesi. Memungkinkan pengguna untuk membuat dan menggunakan hanya sesi interaktif yang terkait dengan pengguna. Kebijakan ini juga mencakup izin lain yang diperlukan oleh AWS Glue untuk mengelola sumber daya Glue di layanan lain AWS

`AwsGlueSessionUserRestrictedServiceRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AwsGlueSessionUserRestrictedServiceRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 14 April 2022, 21:30 UTC
- Waktu telah diedit: Agustus 05, 2024, 23:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AwsGlueSessionUserRestrictedServiceRole`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSGrafanaAccountAdministrator

Deskripsi: Menyediakan akses di Amazon Grafana untuk membuat dan mengelola ruang kerja untuk seluruh organisasi.

`AWSGrafanaAccountAdministrator`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSGrafanaAccountAdministrator` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 23 Februari 2021 00:20 UTC
- Waktu yang telah diedit: 15 Februari 2022, 22.36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGrafanaAccountAdministrator`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSGrafanaOrganizationAdmin",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GrafanaIAMGetRolePermission",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Sid" : "AWSGrafanaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "grafana:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GrafanaIAMPassRolePermission",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "grafana.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSGrafanaConsoleReadOnlyAccess

Deskripsi: Akses untuk membaca hanya operasi di Amazon Grafana.

`AWSGrafanaConsoleReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSGrafanaConsoleReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 23 Februari 2021 00:10 UTC
- Waktu yang telah diedit: 15 Februari 2022, 22.30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGrafanaConsoleReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
  "Statement" : [
    {
      "Sid" : "AWSGrafanaConsoleReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "grafana:Describe*",
        "grafana:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSGrafanaWorkspacePermissionManagement

Deskripsi: Hanya menyediakan kemampuan untuk memperbarui izin pengguna dan grup untuk ruang kerja AWS Grafana.

`AWSGrafanaWorkspacePermissionManagement`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSGrafanaWorkspacePermissionManagement` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 23 Februari 2021 00:15 UTC
- Waktu telah diedit: 15 Maret 2023, 22:17 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGrafanaWorkspacePermissionManagement`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSGrafanaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "grafana:DescribeWorkspace",
        "grafana:DescribeWorkspaceAuthentication",
        "grafana:UpdatePermissions",
        "grafana:ListPermissions",
        "grafana:ListWorkspaces"
      ],
      "Resource" : "arn:aws:grafana:*:*:/workspaces*"
    },
    {
      "Sid" : "IAMIdentityCenterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sso:DescribeRegisteredRegions",
        "sso:GetSharedSsoConfiguration",
        "sso:ListDirectoryAssociations",
        "sso:GetManagedApplicationInstance",
        "sso:ListProfiles",
        "sso:AssociateProfile",
        "sso:DisassociateProfile",
        "sso:GetProfile",
        "sso:ListProfileAssociations",
        "sso-directory:DescribeUser",
        "sso-directory:DescribeGroup"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSGrafanaWorkspacePermissionManagementV2

Deskripsi: Menyediakan kemampuan untuk memperbarui izin pengguna dan grup IAM Identity Center (IDC) untuk ruang kerja Grafana yang Dikelola Amazon.

`AWSGrafanaWorkspacePermissionManagementV2`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSGrafanaWorkspacePermissionManagementV2` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 05 Januari 2024, 18:39 UTC
- Waktu telah diedit: 05 Januari 2024, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGrafanaWorkspacePermissionManagementV2`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSGrafanaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "grafana:DescribeWorkspace",
        "grafana:DescribeWorkspaceAuthentication",
        "grafana:UpdatePermissions",
        "grafana:ListPermissions",
        "grafana:ListWorkspaces"
      ],
      "Resource" : "arn:aws:grafana:*:*:/workspaces*"
    },
    {
      "Sid" : "IAMIdentityCenterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sso:DescribeRegisteredRegions",
        "sso:GetSharedSsoConfiguration",
        "sso:ListDirectoryAssociations",
        "sso:GetManagedApplicationInstance",
        "sso:ListProfiles",
        "sso:GetProfile",
        "sso:ListProfileAssociations",
        "sso-directory:DescribeUser",
        "sso-directory:DescribeGroup"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSGreengrassFullAccess

Deskripsi: Kebijakan ini memberikan akses penuh ke konfigurasi AWS Greengrass, tindakan pengelolaan, dan penerapan

`AWSGreengrassFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSGreengrassFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 Mei 2017, 00:47 UTC
- Waktu yang telah diedit: 03 Mei 2017, 00:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGreengrassFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSGreengrassReadOnlyAccess

Deskripsi: Kebijakan ini memberikan akses hanya baca ke konfigurasi AWS Greengrass, tindakan pengelolaan, dan penerapan

`AWSGreengrassReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSGreengrassReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 Oktober 2018, 16:01 UTC
- Waktu telah diedit: 30 Oktober 2018, 16:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGreengrassReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSGreengrassResourceAccessRolePolicy

Deskripsi: Kebijakan untuk peran layanan AWS Greengrass yang memungkinkan akses ke layanan terkait termasuk Lambda AWS dan IoT thing shadow. AWS

`AWSGreengrassResourceAccessRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSGreengrassResourceAccessRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 14 Februari 2017, 21:17 UTC

- Waktu telah diedit: 14 November 2018, 00:35 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSGreengrassResourceAccessRolePolicy`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowGreengrassAccessToShadows",
      "Action" : [
        "iot:DeleteThingShadow",
        "iot:GetThingShadow",
        "iot:UpdateThingShadow"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iot:*:*:thing/GG_*",
        "arn:aws:iot:*:*:thing/*-gcm",
        "arn:aws:iot:*:*:thing/*-gda",
        "arn:aws:iot:*:*:thing/*-gci"
      ]
    },
    {
      "Sid" : "AllowGreengrassToDescribeThings",
      "Action" : [
        "iot:DescribeThing"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iot:*:*:thing/*"
    },
    {
```

```
      "Sid" : "AllowGreengrassToDescribeCertificates",
      "Action" : [
        "iot:DescribeCertificate"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iot:*:*:cert/*"
    },
    {
      "Sid" : "AllowGreengrassToCallGreengrassServices",
      "Action" : [
        "greengrass:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGreengrassToGetLambdaFunctions",
      "Action" : [
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGreengrassToGetGreengrassSecrets",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:greengrass-*"
    },
    {
      "Sid" : "AllowGreengrassAccessToS3Objects",
      "Action" : [
        "s3:GetObject"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:s3:::*Greengrass*",
        "arn:aws:s3:::*GreenGrass*",
        "arn:aws:s3:::*greengrass*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*SageMaker*",
```

```
        "arn:aws:s3:::*sagemaker*"
      ]
    },
    {
      "Sid" : "AllowGreengrassAccessToS3BucketLocation",
      "Action" : [
        "s3:GetBucketLocation"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGreengrassAccessToSageMakerTrainingJobs",
      "Action" : [
        "sagemaker:DescribeTrainingJob"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-job/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSGroundStationAgentInstancePolicy

Deskripsi: Memberikan izin Instans Titik Akhir Dataflow untuk menggunakan Agen Ground Station AWS

`AWSGroundStationAgentInstancePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSGroundStationAgentInstancePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 Maret 2023, 15:23 UTC
- Waktu telah diedit: 29 Maret 2023, 15:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGroundStationAgentInstancePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSHealth_EventProcessorServiceRolePolicy

Deskripsi: Memungkinkan AWS Kesehatan mengaktifkan fitur prosesor acara Kesehatan.

`AWSHealth_EventProcessorServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 13 Januari 2023, 19:24 UTC
- Waktu telah diedit: 13 Januari 2023, 19:24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSHealth_EventProcessorServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:PutTargets",
        "events:PutRule",
        "events:RemoveTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "event-processor.health.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSHealthFullAccess

Deskripsi: Memungkinkan akses penuh ke API dan Pemberitahuan AWS Kesehatan dan Dasbor Personal Health

`AWSHealthFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSHealthFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Desember 2016, 12:30 UTC
- Waktu yang telah diedit: 16 November 2020, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/AWSHealthFullAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:DisableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "health.amazonaws.com"
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "health:*",
        "organizations:ListAccounts",
        "organizations:ListParents",
        "organizations:DescribeAccount",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "health.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSHealthImagingFullAccess

Deskripsi: Menyediakan akses penuh ke layanan AWS Health Imaging.

`AWSHealthImagingFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSHealthImagingFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 25 Juli 2023, 23:39 UTC
- Waktu telah diedit: 25 Juli 2023, 23:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSHealthImagingFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "medical-imaging:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "medical-imaging.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSHealthImagingReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke layanan AWS Health Imaging.

`AWSHealthImagingReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSHealthImagingReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 25 Juli 2023, 23:40 UTC
- Waktu yang telah diedit: 01 Agustus 2023, 15:18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSHealthImagingReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "medical-imaging:GetDICOMImportJob",
        "medical-imaging:GetDatastore",
        "medical-imaging:GetImageFrame",
        "medical-imaging:GetImageSet",
        "medical-imaging:GetImageSetMetadata",
        "medical-imaging:ListDICOMImportJobs",
        "medical-imaging:ListDatastores",
        "medical-imaging:ListImageSetVersions",
        "medical-imaging:ListTagsForResource",
        "medical-imaging:SearchImageSets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSIAMIdentityCenterAllowListForIdentityContext

Deskripsi: Menyediakan daftar tindakan yang diizinkan untuk peran yang diambil dengan konteks identitas Pusat Identitas IAM. AWS Security Token Service (AWS STS) secara otomatis melampirkan kebijakan ini ke peran yang diasumsikan. Konteks identitas diteruskan sebagai ProvidedContext.

`AWSIAMIdentityCenterAllowListForIdentityContext`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIAMIdentityCenterAllowListForIdentityContext` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 08 November 2023, 15:21 UTC
- Waktu yang telah diedit: 01 Oktober 2024, 14:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIAMIdentityCenterAllowListForIdentityContext`

Versi kebijakan

Versi kebijakan: v12 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSIdentitySyncFullAccess

Deskripsi: Memberikan akses penuh ke layanan Sinkronisasi Identitas

`AWSIdentitySyncFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIdentitySyncFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 23 Maret 2022, 23:29 UTC
- Waktu yang telah diedit: 23 Maret 2022, 23.29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIdentitySyncFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ds:AuthorizeApplication",
        "ds:UnauthorizeApplication"
      ],
      "Resource" : "arn:*:ds:*:*:*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "identity-sync:DeleteSyncProfile",
        "identity-sync:CreateSyncProfile",
        "identity-sync:GetSyncProfile",
        "identity-sync:StartSync",
        "identity-sync:StopSync",
        "identity-sync:CreateSyncFilter",
        "identity-sync:DeleteSyncFilter",
        "identity-sync:ListSyncFilters",
        "identity-sync:CreateSyncTarget",
```

```
        "identity-sync:DeleteSyncTarget",
        "identity-sync:GetSyncTarget",
        "identity-sync:UpdateSyncTarget"
      ],
      "Resource" : "arn:*:identity-sync:*:*:*/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSIdentitySyncReadOnlyAccess

Deskripsi: Akses hanya baca ke layanan Sinkronisasi Identitas

`AWSIdentitySyncReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIdentitySyncReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 23 Maret 2022, 23:29 UTC
- Waktu yang telah diedit: 23 Maret 2022, 23.29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIdentitySyncReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "identity-sync:GetSyncProfile",
        "identity-sync:ListSyncFilters",
        "identity-sync:GetSyncTarget"
      ],
      "Resource" : "arn:*:identity-sync:*:*:*/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSImageBuilderFullAccess

Deskripsi: Menyediakan akses penuh ke semua tindakan AWS Image Builder dan akses cakupan sumber daya ke layanan terkait AWS .

`AWSImageBuilderFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSImageBuilderFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 20 Desember 2019, 18:25 UTC
- Waktu yang telah diedit: 13 April 2021 17.33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSImageBuilderFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "imagebuilder:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : "arn:aws:sns:*:*:*imagebuilder*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "license-manager:ListLicenseConfigurations",
        "license-manager:ListLicenseSpecificationsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/imagebuilder.amazonaws.com/
AWSServiceRoleForImageBuilder"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile"
      ],
      "Resource" : "arn:aws:iam::*:instance-profile/*imagebuilder*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListInstanceProfiles",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:instance-profile/*imagebuilder*",
        "arn:aws:iam::*:role/*imagebuilder*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3::*:*imagebuilder*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/imagebuilder.amazonaws.com/
AWSServiceRoleForImageBuilder",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "imagebuilder.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVpcs",
        "ec2:DescribeRegions",
        "ec2:DescribeVolumes",
        "ec2:DescribeSubnets",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeLaunchTemplates"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSImageBuilderReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke semua tindakan AWS Image Builder.

`AWSImageBuilderReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSImageBuilderReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 19 Desember 2019 22:29 UTC
- Waktu yang telah diedit: 19 Desember 2019, 22:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSImageBuilderReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "imagebuilder:Get*",
        "imagebuilder:List*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/imagebuilder.amazonaws.com/
AWSServiceRoleForImageBuilder"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSImportExportFullAccess

Deskripsi: Menyediakan akses baca dan tulis ke pekerjaan yang dibuat di bawah Akun AWS.

`AWSImportExportFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSImportExportFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu telah diedit: 06 Februari 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSImportExportFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSImportExportReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke pekerjaan yang dibuat di bawah Akun AWS.

`AWSImportExportReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSImportExportReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu telah diedit: 06 Februari 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSImportExportReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSIncidentManagerIncidentAccessServiceRolePolicy

Deskripsi: Memberikan izin Manajer Insiden untuk memanggil AWS layanan lain sebagai bagian dari pengelolaan insiden.

`AWSIncidentManagerIncidentAccessServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIncidentManagerIncidentAccessServiceRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 13 November 2023, 00:01 UTC
- Waktu telah diedit: 20 Februari 2024, 23:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIncidentManagerIncidentAccessServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IncidentAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources",
        "codedeploy:BatchGetDeployments",
        "codedeploy:ListDeployments",
        "codedeploy:ListDeploymentTargets",
        "autoscaling:DescribeAutoScalingInstances"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSIncidentManagerResolverAccess

Deskripsi: Kebijakan ini memberikan izin untuk memulai, melihat, dan memperbarui insiden dengan akses penuh ke peristiwa timeline kustom & item terkait. Tetapkan kebijakan ini kepada pengguna yang akan membuat dan menyelesaikan insiden.

`AWSIncidentManagerResolverAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIncidentManagerResolverAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 10 Mei 2021, 06:12 UTC
- Waktu yang telah diedit: 10 Mei 2021, 06:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIncidentManagerResolverAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "StartIncidentPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-incidents:StartIncident"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ResponsePlanReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-incidents:ListResponsePlans",
        "ssm-incidents:GetResponsePlan"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IncidentRecordResolverPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-incidents:ListIncidentRecords",
        "ssm-incidents:GetIncidentRecord",
        "ssm-incidents:UpdateIncidentRecord",
        "ssm-incidents:ListTimelineEvents",
        "ssm-incidents:CreateTimelineEvent",
        "ssm-incidents:GetTimelineEvent",
        "ssm-incidents:UpdateTimelineEvent",
        "ssm-incidents:DeleteTimelineEvent",
        "ssm-incidents:ListRelatedItems",
        "ssm-incidents:UpdateRelatedItems"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSIncidentManagerServiceRolePolicy

Deskripsi: Kebijakan ini memberikan izin kepada Manajer Insiden untuk mengelola catatan insiden dan sumber daya terkait atas nama Anda.

`AWSIncidentManagerServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 10 Mei 2021, 03:34 UTC
- Waktu telah diedit: 28 Januari 2025, 02:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIncidentManagerServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "UpdateIncidentRecordPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-incidents:ListIncidentRecords",
        "ssm-incidents:CreateTimelineEvent"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RelatedOpsItemPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ssm:CreateOpsItem",
        "ssm:AssociateOpsItemRelatedItem"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IncidentEngagementPermissions",
      "Effect" : "Allow",
      "Action" : "ssm-contacts:StartEngagement",
      "Resource" : "*"
    },
    {
      "Sid" : "PutMetricDataPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/IncidentManager",
            "AWS/Usage"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSIoT1ClickFullAccess

Deskripsi: Menyediakan akses penuh ke AWS IoT 1-Click.

`AWSIoT1ClickFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoT1ClickFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 11 Mei 2018, 22:10 UTC
- Waktu yang telah diedit: 11 Mei 2018, 22:10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoT1ClickFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "iot1click:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSIoT1ClickReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke AWS IoT 1-Klik.

`AWSIoT1ClickReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoT1ClickReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 11 Mei 2018, 21:49 UTC
- Waktu yang telah diedit: 11 Mei 2018, 21:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoT1ClickReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "iot1click:Describe*",
        "iot1click:Get*",
        "iot1click:List*"
      ],
```

```
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSIoTAnalyticsFullAccess

Deskripsi: Menyediakan akses penuh ke IoT Analytics.

`AWSIoTAnalyticsFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoTAnalyticsFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 Juni 2018, 23:02 UTC
- Waktu telah diedit: 18 Juni 2018, 23:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTAnalyticsFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSIoTAnalyticsReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke IoT Analytics.

`AWSIoTAnalyticsReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoTAnalyticsReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 Juni 2018, 21:37 UTC
- Waktu telah diedit: 18 Juni 2018, 21:37 UTC

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

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSIoTConfigAccess

Deskripsi: Kebijakan ini memberikan akses penuh ke tindakan AWS konfigurasi IoT

`AWSIoTConfigAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoTConfigAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Oktober 2015, 21:52 UTC
- Waktu yang telah diedit: 27 September 2019, 20:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTConfigAccess`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:AcceptCertificateTransfer",
        "iot:AddThingToThingGroup",
        "iot:AssociateTargetsWithJob",
        "iot:AttachPolicy",
        "iot:AttachPrincipalPolicy",
        "iot:AttachThingPrincipal",
        "iot:CancelCertificateTransfer",
        "iot:CancelJob",
        "iot:CancelJobExecution",
        "iot:ClearDefaultAuthorizer",
        "iot:CreateAuthorizer",
```

```
        "iot:CreateCertificateFromCsr",
        "iot:CreateJob",
        "iot:CreateKeysAndCertificate",
        "iot:CreateOTAUpdate",
        "iot:CreatePolicy",
        "iot:CreatePolicyVersion",
        "iot:CreateRoleAlias",
        "iot:CreateStream",
        "iot:CreateThing",
        "iot:CreateThingGroup",
        "iot:CreateThingType",
        "iot:CreateTopicRule",
        "iot:DeleteAuthorizer",
        "iot:DeleteCACertificate",
        "iot:DeleteCertificate",
        "iot:DeleteJob",
        "iot:DeleteJobExecution",
        "iot:DeleteOTAUpdate",
        "iot:DeletePolicy",
        "iot:DeletePolicyVersion",
        "iot:DeleteRegistrationCode",
        "iot:DeleteRoleAlias",
        "iot:DeleteStream",
        "iot:DeleteThing",
        "iot:DeleteThingGroup",
        "iot:DeleteThingType",
        "iot:DeleteTopicRule",
        "iot:DeleteV2LoggingLevel",
        "iot:DeprecateThingType",
        "iot:DescribeAuthorizer",
        "iot:DescribeCACertificate",
        "iot:DescribeCertificate",
        "iot:DescribeDefaultAuthorizer",
        "iot:DescribeEndpoint",
        "iot:DescribeEventConfigurations",
        "iot:DescribeIndex",
        "iot:DescribeJob",
        "iot:DescribeJobExecution",
        "iot:DescribeRoleAlias",
        "iot:DescribeStream",
        "iot:DescribeThing",
        "iot:DescribeThingGroup",
        "iot:DescribeThingRegistrationTask",
        "iot:DescribeThingType",
```

```
        "iot:DetachPolicy",
        "iot:DetachPrincipalPolicy",
        "iot:DetachThingPrincipal",
        "iot:DisableTopicRule",
        "iot:EnableTopicRule",
        "iot:GetEffectivePolicies",
        "iot:GetIndexingConfiguration",
        "iot:GetJobDocument",
        "iot:GetLoggingOptions",
        "iot:GetOTAUpdate",
        "iot:GetPolicy",
        "iot:GetPolicyVersion",
        "iot:GetRegistrationCode",
        "iot:GetTopicRule",
        "iot:GetV2LoggingOptions",
        "iot:ListAttachedPolicies",
        "iot:ListAuthorizers",
        "iot:ListCACertificates",
        "iot:ListCertificates",
        "iot:ListCertificatesByCA",
        "iot:ListIndices",
        "iot:ListJobExecutionsForJob",
        "iot:ListJobExecutionsForThing",
        "iot:ListJobs",
        "iot:ListOTAUpdates",
        "iot:ListOutgoingCertificates",
        "iot:ListPolicies",
        "iot:ListPolicyPrincipals",
        "iot:ListPolicyVersions",
        "iot:ListPrincipalPolicies",
        "iot:ListPrincipalThings",
        "iot:ListRoleAliases",
        "iot:ListStreams",
        "iot:ListTargetsForPolicy",
        "iot:ListThingGroups",
        "iot:ListThingGroupsForThing",
        "iot:ListThingPrincipals",
        "iot:ListThingRegistrationTaskReports",
        "iot:ListThingRegistrationTasks",
        "iot:ListThings",
        "iot:ListThingsInThingGroup",
        "iot:ListThingTypes",
        "iot:ListTopicRules",
        "iot:ListV2LoggingLevels",
```

```
        "iot:RegisterCACertificate",
        "iot:RegisterCertificate",
        "iot:RegisterThing",
        "iot:RejectCertificateTransfer",
        "iot:RemoveThingFromThingGroup",
        "iot:ReplaceTopicRule",
        "iot:SearchIndex",
        "iot:SetDefaultAuthorizer",
        "iot:SetDefaultPolicyVersion",
        "iot:SetLoggingOptions",
        "iot:SetV2LoggingLevel",
        "iot:SetV2LoggingOptions",
        "iot:StartThingRegistrationTask",
        "iot:StopThingRegistrationTask",
        "iot:TestAuthorization",
        "iot:TestInvokeAuthorizer",
        "iot:TransferCertificate",
        "iot:UpdateAuthorizer",
        "iot:UpdateCACertificate",
        "iot:UpdateCertificate",
        "iot:UpdateEventConfigurations",
        "iot:UpdateIndexingConfiguration",
        "iot:UpdateRoleAlias",
        "iot:UpdateStream",
        "iot:UpdateThing",
        "iot:UpdateThingGroup",
        "iot:UpdateThingGroupsForThing",
        "iot:UpdateAccountAuditConfiguration",
        "iot:DescribeAccountAuditConfiguration",
        "iot:DeleteAccountAuditConfiguration",
        "iot:StartOnDemandAuditTask",
        "iot:CancelAuditTask",
        "iot:DescribeAuditTask",
        "iot:ListAuditTasks",
        "iot:CreateScheduledAudit",
        "iot:UpdateScheduledAudit",
        "iot:DeleteScheduledAudit",
        "iot:DescribeScheduledAudit",
        "iot:ListScheduledAudits",
        "iot:ListAuditFindings",
        "iot:CreateSecurityProfile",
        "iot:DescribeSecurityProfile",
        "iot:UpdateSecurityProfile",
        "iot:DeleteSecurityProfile",
```

```
        "iot:AttachSecurityProfile",
        "iot:DetachSecurityProfile",
        "iot:ListSecurityProfiles",
        "iot:ListSecurityProfilesForTarget",
        "iot:ListTargetsForSecurityProfile",
        "iot:ListActiveViolations",
        "iot:ListViolationEvents",
        "iot:ValidateSecurityProfileBehaviors"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSIoTConfigReadOnlyAccess

Deskripsi: Kebijakan ini memberikan akses hanya baca ke tindakan AWS konfigurasi IoT

`AWSIoTConfigReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoTConfigReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Oktober 2015, 21:52 UTC
- Waktu yang telah diedit: 27 September 2019, 20:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTConfigReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:DescribeAuthorizer",
        "iot:DescribeCACertificate",
        "iot:DescribeCertificate",
        "iot:DescribeDefaultAuthorizer",
        "iot:DescribeEndpoint",
        "iot:DescribeEventConfigurations",
        "iot:DescribeIndex",
        "iot:DescribeJob",
        "iot:DescribeJobExecution",
        "iot:DescribeRoleAlias",
        "iot:DescribeStream",
        "iot:DescribeThing",
        "iot:DescribeThingGroup",
        "iot:DescribeThingRegistrationTask",
        "iot:DescribeThingType",
        "iot:GetEffectivePolicies",
        "iot:GetIndexingConfiguration",
        "iot:GetJobDocument",
        "iot:GetLoggingOptions",
        "iot:GetOTAUpdate",
        "iot:GetPolicy",
        "iot:GetPolicyVersion",
        "iot:GetRegistrationCode",
        "iot:GetTopicRule",
        "iot:GetV2LoggingOptions",
        "iot:ListAttachedPolicies",
        "iot:ListAuthorizers",
```

```
        "iot:ListCACertificates",
        "iot:ListCertificates",
        "iot:ListCertificatesByCA",
        "iot:ListIndices",
        "iot:ListJobExecutionsForJob",
        "iot:ListJobExecutionsForThing",
        "iot:ListJobs",
        "iot:ListOTAUpdates",
        "iot:ListOutgoingCertificates",
        "iot:ListPolicies",
        "iot:ListPolicyPrincipals",
        "iot:ListPolicyVersions",
        "iot:ListPrincipalPolicies",
        "iot:ListPrincipalThings",
        "iot:ListRoleAliases",
        "iot:ListStreams",
        "iot:ListTargetsForPolicy",
        "iot:ListThingGroups",
        "iot:ListThingGroupsForThing",
        "iot:ListThingPrincipals",
        "iot:ListThingRegistrationTaskReports",
        "iot:ListThingRegistrationTasks",
        "iot:ListThings",
        "iot:ListThingsInThingGroup",
        "iot:ListThingTypes",
        "iot:ListTopicRules",
        "iot:ListV2LoggingLevels",
        "iot:SearchIndex",
        "iot:TestAuthorization",
        "iot:TestInvokeAuthorizer",
        "iot:DescribeAccountAuditConfiguration",
        "iot:DescribeAuditTask",
        "iot:ListAuditTasks",
        "iot:DescribeScheduledAudit",
        "iot:ListScheduledAudits",
        "iot:ListAuditFindings",
        "iot:DescribeSecurityProfile",
        "iot:ListSecurityProfiles",
        "iot:ListSecurityProfilesForTarget",
        "iot:ListTargetsForSecurityProfile",
        "iot:ListActiveViolations",
        "iot:ListViolationEvents",
        "iot:ValidateSecurityProfileBehaviors"
      ],
```

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSIoTDataAccess

Deskripsi: Kebijakan ini memberikan akses penuh ke tindakan AWS pesan IoT

`AWSIoTDataAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoTDataAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Oktober 2015, 21:51 UTC
- Waktu yang telah diedit: 23 Juni 2021 21:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTDataAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:Connect",
        "iot:Publish",
        "iot:Subscribe",
        "iot:Receive",
        "iot:GetThingShadow",
        "iot:UpdateThingShadow",
        "iot:DeleteThingShadow",
        "iot:ListNamedShadowsForThing"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction

Deskripsi: Menyediakan akses tulis ke grup hal IoT dan akses baca ke Sertifikat IoT untuk eksekusi tindakan mitigasi ADD_THINGS_TO_THING_GROUP

`AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 07 Agustus 2019, 17:55 UTC
- Waktu yang telah diedit: 07 Agustus 2019, 17:55 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSIoTDeviceDefenderAudit

Deskripsi: Menyediakan akses baca untuk IoT dan sumber daya terkait

`AWSIoTDeviceDefenderAudit`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoTDeviceDefenderAudit` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 18 Juli 2018, 21:17 UTC
- Waktu yang telah diedit: 25 November 2019, 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderAudit`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:GetLoggingOptions",
        "iot:GetV2LoggingOptions",
        "iot:ListCACertificates",
        "iot:ListCertificates",
        "iot:DescribeCACertificate",
        "iot:DescribeCertificate",
        "iot:ListPolicies",
        "iot:GetPolicy",
        "iot:GetEffectivePolicies",
        "iot:ListRoleAliases",
        "iot:DescribeRoleAlias",
        "cognito-identity:GetIdentityPoolRoles",
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies",
        "iam:GetRole",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRolePolicy",
        "iam:GenerateServiceLastAccessedDetails",
        "iam:GetServiceLastAccessedDetails"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction

Deskripsi: Menyediakan akses untuk mengaktifkan pencatatan IoT untuk eksekusi tindakan mitigasi ENABLE_IOT_LOGGING

`AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 07 Agustus 2019, 17:04 UTC
- Waktu yang telah diedit: 07 Agustus 2019, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
        "iot:SetV2LoggingOptions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "iot.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction

Deskripsi: Menyediakan pesan mempublikasikan akses ke topik SNS untuk eksekusi tindakan mitigasi PUBLISH_FINDING_TO_SNS

`AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 07 Agustus 2019, 17:04 UTC
- Waktu yang telah diedit: 07 Agustus 2019, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction

Deskripsi: Menyediakan akses tulis ke kebijakan IoT untuk eksekusi tindakan mitigasi REPLACE_DEFAULT_POLICY_VERSION

`AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 07 Agustus 2019, 17:04 UTC
- Waktu yang telah diedit: 07 Agustus 2019, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSIoTDeviceDefenderUpdateCACertMitigationAction

Deskripsi: Menyediakan akses tulis ke sertifikat IoT CA untuk eksekusi tindakan mitigasi UPDATE_CA_CERTIFICATE

`AWSIoTDeviceDefenderUpdateCACertMitigationAction`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoTDeviceDefenderUpdateCACertMitigationAction` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 07 Agustus 2019, 17:05 UTC
- Waktu yang telah diedit: 07 Agustus 2019, 17:05 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderUpdateCACertMitigationAction`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction

Deskripsi: Menyediakan akses tulis ke sertifikat IoT untuk eksekusi tindakan mitigasi UPDATE_DEVICE_CERTIFICATE

`AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 07 Agustus 2019, 17:06 UTC
- Waktu yang telah diedit: 07 Agustus 2019, 17:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:UpdateCertificate"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSIoTDeviceTesterForFreeRTOSFullAccess

Deskripsi: Mengizinkan Penguji Perangkat AWS IoT menjalankan rangkaian kualifikasi FreeRTOS dengan mengizinkan akses ke layanan termasuk IoT, S3, dan IAM

`AWSIoTDeviceTesterForFreeRTOSFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoTDeviceTesterForFreeRTOSFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 12 Februari 2020, 20:33 UTC
- Waktu telah diedit: 10 Agustus 2023, 20:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTDeviceTesterForFreeRTOSFullAccess`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/idt-*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "iot.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "VisualEditor1",
      "Effect" : "Allow",
      "Action" : [
        "iot:DeleteThing",
        "iot:AttachThingPrincipal",
        "iot:DeleteCertificate",
        "iot:GetRegistrationCode",
        "iot:CreatePolicy",
        "iot:UpdateCACertificate",
        "s3:ListBucket",
        "iot:DescribeEndpoint",
        "iot:CreateOTAUpdate",
        "iot:CreateStream",
        "signer:ListSigningJobs",
        "acm:ListCertificates",
        "iot:CreateKeysAndCertificate",
        "iot:UpdateCertificate",
        "iot:CreateCertificateFromCsr",
```

```
        "iot:DetachThingPrincipal",
        "iot:RegisterCACertificate",
        "iot:CreateThing",
        "iam:ListRoles",
        "iot:RegisterCertificate",
        "iot:DeleteCACertificate",
        "signer:PutSigningProfile",
        "s3:ListAllMyBuckets",
        "signer:ListSigningPlatforms",
        "iot-device-tester:SendMetrics",
        "iot-device-tester:SupportedVersion",
        "iot-device-tester:LatestIdt",
        "iot-device-tester:CheckVersion",
        "iot-device-tester:DownloadTestSuite"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor2",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "signer:StartSigningJob",
        "acm:GetCertificate",
        "signer:DescribeSigningJob",
        "s3:CreateBucket",
        "execute-api:Invoke",
        "s3:DeleteBucket",
        "s3:PutBucketVersioning",
        "signer:CancelSigningProfile"
      ],
      "Resource" : [
        "arn:aws:execute-api:us-east-1:098862408343:9xpmnvs5h4/prod/POST/metrics",
        "arn:aws:signer:*:*:/signing-profiles/*",
        "arn:aws:signer:*:*:/signing-jobs/*",
        "arn:aws:iam::*:role/idt-*",
        "arn:aws:acm:*:*:certificate/*",
        "arn:aws:s3:::idt-*",
        "arn:aws:s3:::afr-ota*"
      ]
    },
    {
      "Sid" : "VisualEditor3",
      "Effect" : "Allow",
```

```
      "Action" : [
        "iot:DeleteStream",
        "iot:DeleteCertificate",
        "iot:AttachPolicy",
        "iot:DetachPolicy",
        "iot:DeletePolicy",
        "s3:ListBucketVersions",
        "iot:UpdateCertificate",
        "iot:GetOTAUpdate",
        "iot:DeleteOTAUpdate",
        "iot:DescribeJobExecution"
      ],
      "Resource" : [
        "arn:aws:s3:::afr-ota*",
        "arn:aws:iot:*:*:thinggroup/idt*",
        "arn:aws:iam::*:role/idt-*"
      ]
    },
    {
      "Sid" : "VisualEditor4",
      "Effect" : "Allow",
      "Action" : [
        "iot:DeleteCertificate",
        "iot:AttachPolicy",
        "iot:DetachPolicy",
        "s3:DeleteObjectVersion",
        "iot:DeleteOTAUpdate",
        "s3:PutObject",
        "s3:GetObject",
        "iot:DeleteStream",
        "iot:DeletePolicy",
        "s3:DeleteObject",
        "iot:UpdateCertificate",
        "iot:GetOTAUpdate",
        "s3:GetObjectVersion",
        "iot:DescribeJobExecution"
      ],
      "Resource" : [
        "arn:aws:s3:::afr-ota*/*",
        "arn:aws:s3:::idt-*/*",
        "arn:aws:iot:*:*:policy/idt*",
        "arn:aws:iam::*:role/idt-*",
        "arn:aws:iot:*:*:otaupdate/idt*",
        "arn:aws:iot:*:*:thing/idt*",
```

```
        "arn:aws:iot:*:*:cert/*",
        "arn:aws:iot:*:*:job/*",
        "arn:aws:iot:*:*:stream/*"
      ]
    },
    {
      "Sid" : "VisualEditor5",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::afr-ota*/*",
        "arn:aws:s3:::idt-*/*"
      ]
    },
    {
      "Sid" : "VisualEditor6",
      "Effect" : "Allow",
      "Action" : [
        "iot:CancelJobExecution"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:job/*",
        "arn:aws:iot:*:*:thing/idt*"
      ]
    },
    {
      "Sid" : "VisualEditor7",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/Owner" : "IoTDeviceTester"
        }
      }
    },
    {
```

```
      "Sid" : "VisualEditor8",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/Owner" : "IoTDeviceTester"
        }
      }
    },
    {
      "Sid" : "VisualEditor9",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/Owner" : "IoTDeviceTester"
        }
      }
    },
    {
      "Sid" : "VisualEditor10",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:placement-group/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:network-interface/*",
```

```
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Sid" : "VisualEditor11",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/Owner" : "IoTDeviceTester"
        }
      }
    },
    {
      "Sid" : "VisualEditor12",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups",
        "ssm:DescribeParameters",
        "ssm:GetParameters"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor13",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "Owner"
          ]
```

```
        },
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances",
            "CreateSecurityGroup"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSIoTDeviceTesterForGreengrassFullAccess

Deskripsi: Mengizinkan Penguji Perangkat AWS IoT menjalankan rangkaian kualifikasi Greengrass dengan mengizinkan akses ke layanan terkait AWS termasuk Lambda, IoT, API Gateway, IAM

`AWSIoTDeviceTesterForGreengrassFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoTDeviceTesterForGreengrassFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 20 Februari 2020, 21:21 UTC
- Waktu yang telah diedit: 25 Juni 2020, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTDeviceTesterForGreengrassFullAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor1",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/idt-*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "iot.amazonaws.com",
            "lambda.amazonaws.com",
            "greengrass.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "VisualEditor2",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "iot:DeleteCertificate",
        "lambda:DeleteFunction",
        "execute-api:Invoke",
        "iot:UpdateCertificate"
      ],
      "Resource" : [
        "arn:aws:execute-api:us-east-1:098862408343:9xpmnvs5h4/prod/POST/metrics",
        "arn:aws:lambda:*:*:function:idt-*",
        "arn:aws:iot:*:*:cert/*"
      ]
```

```
    },
    {
      "Sid" : "VisualEditor3",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateThing",
        "iot:DeleteThing"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/idt-*",
        "arn:aws:iot:*:*:cert/*"
      ]
    },
    {
      "Sid" : "VisualEditor4",
      "Effect" : "Allow",
      "Action" : [
        "iot:AttachPolicy",
        "iot:DetachPolicy",
        "iot:DeletePolicy"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:policy/idt-*",
        "arn:aws:iot:*:*:cert/*"
      ]
    },
    {
      "Sid" : "VisualEditor5",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateJob",
        "iot:DescribeJob",
        "iot:DescribeJobExecution",
        "iot:DeleteJob"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/idt-*",
        "arn:aws:iot:*:*:job/*"
      ]
    },
    {
      "Sid" : "VisualEditor6",
      "Effect" : "Allow",
      "Action" : [
```

```
        "iot:DescribeEndpoint",
        "greengrass:*",
        "iam:ListAttachedRolePolicies",
        "iot:CreatePolicy",
        "iot:GetThingShadow",
        "iot:CreateKeysAndCertificate",
        "iot:ListThings",
        "iot:UpdateThingShadow",
        "iot:CreateCertificateFromCsr",
        "iot-device-tester:SendMetrics",
        "iot-device-tester:SupportedVersion",
        "iot-device-tester:LatestIdt",
        "iot-device-tester:CheckVersion",
        "iot-device-tester:DownloadTestSuite"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor7",
      "Effect" : "Allow",
      "Action" : [
        "iot:DetachThingPrincipal",
        "iot:AttachThingPrincipal"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/idt-*",
        "arn:aws:iot:*:*:cert/*"
      ]
    },
    {
      "Sid" : "VisualEditor8",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:DeleteObjectVersion",
        "s3:ListBucketVersions",
        "s3:CreateBucket",
        "s3:DeleteObject",
        "s3:DeleteBucket"
      ],
      "Resource" : "arn:aws:s3:::idt*"
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSIoTEventsFullAccess

Deskripsi: Menyediakan akses penuh ke IoT Events.

`AWSIoTEventsFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoTEventsFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 10 Januari 2019, 22:51 UTC
- Waktu yang telah diedit: 10 Januari 2019, 22:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTEventsFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSIoTEventsReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke IoT Events.

`AWSIoTEventsReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoTEventsReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 10 Januari 2019, 22:50 UTC
- Waktu yang telah diedit: 23 September 2019, 17:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTEventsReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSIoTFleetHubFederationAccess

Deskripsi: Akses Federasi untuk aplikasi IoT Fleet Hub

`AWSIoTFleetHubFederationAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoTFleetHubFederationAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 15 Desember 2020, 08:08 UTC
- Waktu yang telah diedit: 04 April 2022, 18.03 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTFleetHubFederationAccess`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:DescribeIndex",
        "iot:DescribeThingGroup",
        "iot:GetBucketsAggregation",
        "iot:GetCardinality",
        "iot:GetIndexingConfiguration",
        "iot:GetPercentiles",
        "iot:GetStatistics",
        "iot:SearchIndex",
        "iot:CreateFleetMetric",
        "iot:ListFleetMetrics",
        "iot:DeleteFleetMetric",
        "iot:DescribeFleetMetric",
```

```
        "iot:UpdateFleetMetric",
        "iot:DescribeCustomMetric",
        "iot:ListCustomMetrics",
        "iot:ListDimensions",
        "iot:ListMetricValues",
        "iot:ListThingGroups",
        "iot:ListThingsInThingGroup",
        "iot:ListJobTemplates",
        "iot:DescribeJobTemplate",
        "iot:ListJobs",
        "iot:CreateJob",
        "iot:CancelJob",
        "iot:DescribeJob",
        "iot:ListJobExecutionsForJob",
        "iot:ListJobExecutionsForThing",
        "iot:DescribeJobExecution",
        "iot:ListSecurityProfiles",
        "iot:DescribeSecurityProfile",
        "iot:ListActiveViolations",
        "iot:GetThingShadow",
        "iot:ListNamedShadowsForThing",
        "iot:CancelJobExecution",
        "iot:DescribeEndpoint",
        "iotfleethub:DescribeApplication",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics",
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:DeleteTopic",
        "sns:ListSubscriptionsByTopic",
        "sns:Subscribe",
        "sns:Unsubscribe"
      ],
      "Resource" : "arn:aws:sns:*:*:iotfleethub*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarmHistory"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:iotfleethub*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSIoTFleetwiseServiceRolePolicy

Deskripsi: Memberikan izin ke AWS Sumber Daya dan MetaData yang digunakan atau dikelola oleh untuk fitur tambahan AWSIo TFleetwise

`AWSIoTFleetwiseServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 21 September 2022, 23:27 UTC
- Waktu yang telah diedit: 21 September 2022, 23.27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTFleetwiseServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSIoTFullAccess

Deskripsi: Kebijakan ini memberikan akses penuh ke konfigurasi AWS IoT dan tindakan pengiriman pesan

`AWSIoTFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoTFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 08 Oktober 2015, 15:19 UTC
- Waktu yang telah diedit: 19 Mei 2022 21.39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSIoTLogging

Deskripsi: Memungkinkan pembuatan grup Amazon CloudWatch Log dan streaming log ke grup

`AWSIoTLogging`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoTLogging` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 08 Oktober 2015, 15:17 UTC
- Waktu telah diedit: 08 Oktober 2015, 15:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTLogging`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:PutMetricFilter",
        "logs:PutRetentionPolicy",
        "logs:GetLogEvents",
        "logs:DeleteLogStream"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSIoTManagedIntegrationsFullAccess

Deskripsi: Menyediakan akses penuh ke integrasi terkelola untuk AWS IoT Device Management dan layanan terkait.

`AWSIoTManagedIntegrationsFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoTManagedIntegrationsFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 05 Maret 2025, 19:22 UTC
- Waktu telah diedit: 05 Maret 2025, 19:22 UTC

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

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSIoTManagedIntegrationsRolePolicy

Deskripsi: Menyediakan integrasi terkelola untuk izin AWS IoT Device Management untuk mempublikasikan log dan metrik atas nama Anda.

`AWSIoTManagedIntegrationsRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 05 Maret 2025, 21:22 UTC
- Waktu telah diedit: 05 Maret 2025, 21:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTManagedIntegrationsRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSIoTOTAUpdate

Deskripsi: Memungkinkan akses untuk membuat AWS IoT Job dan menjelaskan pekerjaan penandatangan AWS kode

`AWSIoTOTAUpdate`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoTOTAUpdate` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 20 Desember 2017, 20:36 UTC
- Waktu telah diedit: 20 Desember 2017, 20:36 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTOTAUpdate`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
    "Effect" : "Allow",
    "Action" : [
      "iot:CreateJob",
      "signer:DescribeSigningJob"
    ],
    "Resource" : "*"
  }
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSIotRoboRunnerFullAccess

Deskripsi: Kebijakan ini memberikan izin yang memungkinkan akses penuh ke AWS IOT. RoboRunner

`AWSIotRoboRunnerFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIotRoboRunnerFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 November 2021 03:54 UTC
- Waktu telah diedit: 23 Februari 2023, 18:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIotRoboRunnerFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSIotRoboRunnerReadOnly

Deskripsi: Kebijakan ini memberikan izin yang memungkinkan akses hanya-baca ke Iot. AWS RoboRunner

`AWSIotRoboRunnerReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIotRoboRunnerReadOnly` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 November 2021, 03:43 UTC
- Waktu yang telah diedit: 16 November 2022, 20.51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIotRoboRunnerReadOnly`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotroborunner:GetSite",
        "iotroborunner:GetWorker",
        "iotroborunner:ListWorkerFleets",
        "iotroborunner:ListSites",
        "iotroborunner:ListWorkers",
        "iotroborunner:GetDestination",
        "iotroborunner:GetWorkerFleet",
        "iotroborunner:ListDestinations"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSIotRoboRunnerServiceRolePolicy

Deskripsi: Memungkinkan AWS IoT RoboRunner mengelola AWS Sumber Daya terkait atas nama pelanggan.

`AWSIotRoboRunnerServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 21 Februari 2023, 16:56 UTC
- Waktu yang telah diedit: 21 Februari 2023, 16:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIotRoboRunnerServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSIoTRuleActions

Deskripsi: Memungkinkan akses ke semua AWS layanan yang didukung dalam AWS Tindakan Aturan IoT

`AWSIoTRuleActions`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoTRuleActions` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 08 Oktober 2015, 15:14 UTC
- Waktu telah diedit: 16 Januari 2018, 19:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTRuleActions`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "dynamodb:PutItem",
      "kinesis:PutRecord",
      "iot:Publish",
      "s3:PutObject",
      "sns:Publish",
      "sqs:SendMessage*",
      "cloudwatch:SetAlarmState",
      "cloudwatch:PutMetricData",
      "es:ESHttpPut",
      "firehose:PutRecord"
    ],
    "Resource" : "*"
  }
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSIoTSiteWiseConsoleFullAccess

Deskripsi: Menyediakan akses penuh untuk mengelola AWS IoT SiteWise menggunakan file. AWS Management Console Perhatikan bahwa kebijakan ini juga memberikan akses untuk membuat dan mencantumkan penyimpanan data yang digunakan dengan AWS IoT (AWS misalnya SiteWise IoT Analytics), akses ke daftar dan tampilan sumber daya AWS IoT Greengrass, membuat daftar dan memodifikasi AWS rahasia Secrets Manager, mengambil bayangan IoT, mencantumkan sumber daya dengan tag AWS tertentu, serta membuat serta menggunakan peran terkait layanan untuk IoT. AWS SiteWise

`AWSIoTSiteWiseConsoleFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoTSiteWiseConsoleFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 31 Mei 2019, 21:37 UTC
- Waktu yang telah diedit: 31 Mei 2019, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTSiteWiseConsoleFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : "iotsitewise:*",
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "iotanalytics:List*",
        "iotanalytics:Describe*",
        "iotanalytics:Create*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "iot:DescribeEndpoint",
        "iot:GetThingShadow"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "greengrass:GetGroup",
        "greengrass:GetGroupVersion",
        "greengrass:GetCoreDefinitionVersion",
        "greengrass:ListGroups"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "secretsmanager:ListSecrets",
        "secretsmanager:CreateSecret"
      ],
      "Effect" : "Allow",
```

```
      "Resource" : "*"
    },
    {
      "Action" : [
        "secretsmanager:UpdateSecret"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:greengrass-*"
    },
    {
      "Action" : [
        "tag:GetResources"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/iotsitewise.amazonaws.com/
AWSServiceRoleForIoTSiteWise*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "iotsitewise.amazonaws.com"
        }
      }
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/iotsitewise.amazonaws.com/
AWSServiceRoleForIoTSiteWise*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "iotsitewise.amazonaws.com"
        }
      }
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSIoTSiteWiseFullAccess

Deskripsi: Menyediakan akses penuh ke IoT SiteWise.

`AWSIoTSiteWiseFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoTSiteWiseFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 04 Desember 2018, 20:53 UTC
- Waktu telah diedit: 04 Desember 2018, 20:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTSiteWiseFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSIoTSiteWiseMonitorPortalAccess

Deskripsi: Kebijakan ini memberikan izin untuk mengakses aset AWS IoT dan data SiteWise aset, membuat sumber daya SiteWise Monitor AWS IoT, dan membuat daftar pengguna SSO. AWS

`AWSIoTSiteWiseMonitorPortalAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoTSiteWiseMonitorPortalAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 19 Mei 2020, 20:01 UTC
- Waktu yang telah diedit: 19 Mei 2020, 20:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTSiteWiseMonitorPortalAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotsitewise:CreateProject",
        "iotsitewise:DescribeProject",
        "iotsitewise:UpdateProject",
        "iotsitewise:DeleteProject",
        "iotsitewise:ListProjects",
        "iotsitewise:BatchAssociateProjectAssets",
        "iotsitewise:BatchDisassociateProjectAssets",
        "iotsitewise:ListProjectAssets",
        "iotsitewise:CreateDashboard",
        "iotsitewise:DescribeDashboard",
        "iotsitewise:UpdateDashboard",
        "iotsitewise:DeleteDashboard",
        "iotsitewise:ListDashboards",
        "iotsitewise:CreateAccessPolicy",
        "iotsitewise:DescribeAccessPolicy",
        "iotsitewise:UpdateAccessPolicy",
        "iotsitewise:DeleteAccessPolicy",
        "iotsitewise:ListAccessPolicies",
        "iotsitewise:DescribeAsset",
        "iotsitewise:ListAssets",
        "iotsitewise:ListAssociatedAssets",
        "iotsitewise:DescribeAssetProperty",
        "iotsitewise:GetAssetPropertyValue",
        "iotsitewise:GetAssetPropertyValueHistory",
        "iotsitewise:GetAssetPropertyAggregates",
        "sso-directory:DescribeUsers"
      ],
```

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSIoTSiteWiseMonitorServiceRolePolicy

Deskripsi: Peran ini memberikan izin monitor AWS SiteWise IoT untuk mengakses aset & properti aset AWS SiteWise IoT Anda, dan membuat proyek, dasbor & kebijakan akses AWS IoT Sitewise melalui portal IoT. AWS SiteWise

`AWSIoTSiteWiseMonitorServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 14 November 2019 00:59 UTC
- Waktu yang telah diedit: 13 Desember 2019, 22:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTSiteWiseMonitorServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotsitewise:CreateProject",
        "iotsitewise:DescribeProject",
        "iotsitewise:UpdateProject",
        "iotsitewise:DeleteProject",
        "iotsitewise:ListProjects",
        "iotsitewise:BatchAssociateProjectAssets",
        "iotsitewise:BatchDisassociateProjectAssets",
        "iotsitewise:ListProjectAssets",
        "iotsitewise:CreateDashboard",
        "iotsitewise:DescribeDashboard",
        "iotsitewise:UpdateDashboard",
        "iotsitewise:DeleteDashboard",
        "iotsitewise:ListDashboards",
        "iotsitewise:CreateAccessPolicy",
        "iotsitewise:DescribeAccessPolicy",
        "iotsitewise:UpdateAccessPolicy",
        "iotsitewise:DeleteAccessPolicy",
        "iotsitewise:ListAccessPolicies",
        "iotsitewise:DescribeAsset",
        "iotsitewise:ListAssets",
        "iotsitewise:ListAssociatedAssets",
        "iotsitewise:DescribeAssetProperty",
        "iotsitewise:GetAssetPropertyValue",
        "iotsitewise:GetAssetPropertyValueHistory",
        "iotsitewise:GetAssetPropertyAggregates",
        "sso-directory:DescribeUsers"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSIoTSiteWiseReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke IoT SiteWise.

`AWSIoTSiteWiseReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoTSiteWiseReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 04 Desember 2018, 20:55 UTC
- Waktu yang telah diedit: 16 September 2022, 19.05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTSiteWiseReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotsitewise:Describe*",
        "iotsitewise:List*",
        "iotsitewise:Get*",
        "iotsitewise:BatchGet*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSIoTThingsRegistration

Deskripsi: Kebijakan ini memungkinkan pengguna untuk mendaftarkan berbagai hal secara massal menggunakan AWS IoT API StartThingRegistrationTask

`AWSIoTThingsRegistration`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoTThingsRegistration` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 01 Desember 2017, 20:21 UTC
- Waktu yang telah diedit: 05 Oktober 2020, 19:20 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTThingsRegistration`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:AddThingToThingGroup",
        "iot:AttachPolicy",
        "iot:AttachPrincipalPolicy",
        "iot:AttachThingPrincipal",
        "iot:CreateCertificateFromCsr",
        "iot:CreatePolicy",
        "iot:CreateThing",
        "iot:DescribeCertificate",
        "iot:DescribeThing",
        "iot:DescribeThingGroup",
        "iot:DescribeThingType",
        "iot:DetachPolicy",
        "iot:DetachThingPrincipal",
        "iot:GetPolicy",
        "iot:ListAttachedPolicies",
        "iot:ListPolicyPrincipals",
        "iot:ListPrincipalPolicies",
        "iot:ListPrincipalThings",
        "iot:ListTargetsForPolicy",
        "iot:ListThingGroupsForThing",
        "iot:ListThingPrincipals",
        "iot:RegisterCertificate",
        "iot:RegisterThing",
        "iot:RemoveThingFromThingGroup",
        "iot:UpdateCertificate",
        "iot:UpdateThing",
        "iot:UpdateThingGroupsForThing",
```

```
        "iot:AddThingToBillingGroup",
        "iot:DescribeBillingGroup",
        "iot:RemoveThingFromBillingGroup"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSIoTTwinMakerServiceRolePolicy

Deskripsi: Memungkinkan AWS IoT TwinMaker untuk memanggil AWS layanan lain dan menyinkronkan sumber daya mereka atas nama Anda.

`AWSIoTTwinMakerServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 13 November 2023, 18:59 UTC
- Waktu telah diedit: 13 November 2023, 18:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTTwinMakerServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SiteWiseAssetReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "iotsitewise:DescribeAsset"
      ],
      "Resource" : [
        "arn:aws:iotsitewise:*:*:asset/*"
      ]
    },
    {
      "Sid" : "SiteWiseAssetModelReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "iotsitewise:DescribeAssetModel"
      ],
      "Resource" : [
        "arn:aws:iotsitewise:*:*:asset-model/*"
      ]
    },
    {
      "Sid" : "SiteWiseAssetModelAndAssetListAccess",
      "Effect" : "Allow",
      "Action" : [
        "iotsitewise:ListAssets",
        "iotsitewise:ListAssetModels"
      ],
      "Resource" : [
        "*"
      ]
```

```
    },
    {
      "Sid" : "TwinMakerAccess",
      "Effect" : "Allow",
      "Action" : [
        "iottwinmaker:GetEntity",
        "iottwinmaker:CreateEntity",
        "iottwinmaker:UpdateEntity",
        "iottwinmaker:DeleteEntity",
        "iottwinmaker:ListEntities",
        "iottwinmaker:GetComponentType",
        "iottwinmaker:CreateComponentType",
        "iottwinmaker:UpdateComponentType",
        "iottwinmaker:DeleteComponentType",
        "iottwinmaker:ListComponentTypes"
      ],
      "Resource" : [
        "arn:aws:iottwinmaker:*:*:workspace/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "iottwinmaker:linkedServices" : [
            "IOTSITEWISE"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSIoTWirelessDataAccess

Deskripsi: Memungkinkan akses data identitas terkait ke perangkat AWS IoT Wireless.

`AWSIoTWirelessDataAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoTWirelessDataAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 15 Desember 2020 15:31 UTC
- Waktu yang telah diedit: 15 Desember 2020, 15:31 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessDataAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSIoTWirelessFullAccess

Deskripsi: Memungkinkan identitas terkait akses penuh ke semua operasi AWS IoT Wireless.

`AWSIoTWirelessFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoTWirelessFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 15 Desember 2020 15:27 UTC
- Waktu yang telah diedit: 15 Desember 2020, 15:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSIoTWirelessFullPublishAccess

Deskripsi: Menyediakan akses penuh IoT Wireless untuk mempublikasikan ke IoT Rules Engine atas nama Anda.

`AWSIoTWirelessFullPublishAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoTWirelessFullPublishAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 15 Desember 2020 15:29 UTC
- Waktu yang telah diedit: 15 Desember 2020, 15:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessFullPublishAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSIoTWirelessGatewayCertManager

Deskripsi: Memungkinkan akses identitas terkait untuk membuat, membuat daftar, dan mendeskripsikan Sertifikat IoT

`AWSIoTWirelessGatewayCertManager`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoTWirelessGatewayCertManager` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 15 Desember 2020, 15:30 UTC
- Waktu yang telah diedit: 15 Desember 2020, 15:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessGatewayCertManager`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IoTWirelessGatewayCertManager",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateKeysAndCertificate",
        "iot:DescribeCertificate",
        "iot:ListCertificates"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSIoTWirelessLogging

Deskripsi: Memungkinkan identitas terkait untuk membuat grup Amazon CloudWatch Logs dan mengalirkan log ke grup.

`AWSIoTWirelessLogging`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoTWirelessLogging` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 15 Desember 2020 15:32 UTC
- Waktu yang telah diedit: 15 Desember 2020, 15:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessLogging`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
        "logs:CreateLogStream",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/iotwireless*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSIoTWirelessReadOnlyAccess

Deskripsi: Memungkinkan akses hanya baca identitas terkait ke nirkabel AWS IoT.

`AWSIoTWirelessReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoTWirelessReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 15 Desember 2020 15:28 UTC
- Waktu yang telah diedit: 15 Desember 2020, 15:28 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSIPAMServiceRolePolicy

Deskripsi: Memungkinkan VPC IP Address Manager untuk mengakses sumber daya VPC dan berintegrasi dengan AWS Organizations atas nama Anda.

`AWSIPAMServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 30 November 2021, 19:08 UTC
- Waktu telah diedit: November 08, 2024, 16:29 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIPAMServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IPAMDiscoveryDescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeByoipCidrs",
        "ec2:DescribeIpv6Pools",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePublicIpv4Pools",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:GetIpamDiscoveredAccounts",
        "ec2:GetIpamDiscoveredPublicAddresses",
        "ec2:GetIpamDiscoveredResourceCidrs",
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListByoipCidrs",
```

```
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:DescribeOrganizationalUnit"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchMetricsPublishActions",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/IPAM"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSIQContractServiceRolePolicy

Deskripsi: Digunakan oleh AWS IQ untuk melaksanakan permintaan pembayaran atas nama pelanggan

`AWSIQContractServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 22 Agustus 2019 19:28 UTC
- Waktu yang telah diedit: 22 Agustus 2019, 19:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIQContractServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSIQFullAccess

Deskripsi: Menyediakan akses penuh ke AWS IQ

`AWSIQFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIQFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 04 April 2019, 23:13 UTC
- Waktu yang telah diedit: 25 September 2019, 20:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIQFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "permission.iq.amazonaws.com",
            "contract.iq.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSIQPermissionServiceRolePolicy

Deskripsi: Memungkinkan AWS IQ untuk mengelola peran yang diasumsikan oleh para ahli IQ AWS .

`AWSIQPermissionServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 22 Agustus 2019 19:36 UTC

- Waktu yang telah diedit: 22 Agustus 2019, 19:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIQPermissionServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : "arn:aws:iam::*:role/AWSIQPermission-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/AWSIQPermission-*",
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : "arn:aws:iam::aws:policy/AWSDenyAll"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DetachRolePolicy"
```

```
      ],
      "Resource" : "arn:aws:iam::*:role/AWSIQPermission-*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy

Deskripsi: Memungkinkan akses ke AWS layanan dan sumber daya yang diperlukan untuk toko kunci kustom AWS KMS

`AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 14 November 2018, 20:10 UTC
- Waktu telah diedit: 10 November 2023, 19:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudhsm:Describe*",
        "ec2:CreateNetworkInterface",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy

Deskripsi: Mengaktifkan AWS KMS untuk menyinkronkan properti bersama kunci Multi-region.

`AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 16 Juni 2021, 15:37 UTC
- Waktu telah diedit: 13 November 2024, 22:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSKeyManagementServicePowerUser

Deskripsi: Menyediakan akses ke Layanan Manajemen AWS Kunci (KMS).

`AWSKeyManagementServicePowerUser`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSKeyManagementServicePowerUser` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu diedit: 07 Maret 2017, 00:55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSKeyManagementServicePowerUser`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateAlias",
        "kms:CreateKey",
        "kms:DeleteAlias",
        "kms:Describe*",
        "kms:GenerateRandom",
        "kms:Get*",
        "kms:List*",
        "kms:TagResource",
        "kms:UntagResource",
        "iam:ListGroups",
        "iam:ListRoles",
        "iam:ListUsers"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSLakeFormationCrossAccountManager

Deskripsi: Menyediakan akses lintas akun ke sumber daya Glue melalui Lake Formation. Juga memberikan akses baca ke layanan lain yang diperlukan seperti organisasi dan manajer akses sumber daya

`AWSLakeFormationCrossAccountManager`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSLakeFormationCrossAccountManager` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 04 Agustus 2020, 20:59 UTC
- Waktu yang telah diedit: 25 Februari 2025, 00:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLakeFormationCrossAccountManager`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSLakeFormationDataAdmin

Deskripsi: Memberikan akses administratif ke AWS Lake Formation dan layanan terkait, seperti AWS Glue, untuk mengelola data lake

`AWSLakeFormationDataAdmin`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSLakeFormationDataAdmin` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 08 Agustus 2019, 17:33 UTC
- Waktu yang telah diedit: 03 Desember 2024, 15:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLakeFormationDataAdmin`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSLambda_FullAccess

Deskripsi: Memberikan akses penuh ke layanan AWS Lambda, fitur konsol AWS Lambda, dan layanan terkait lainnya. AWS

`AWSLambda_FullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSLambda_FullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 17 November 2020, 21:14 UTC
- Waktu telah diedit: 17 Maret 2025, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambda_FullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricData",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "kms:ListAliases",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
```

```
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "lambda:*",
        "logs:DescribeLogGroups",
        "states:DescribeStateMachine",
        "states:ListStateMachines",
        "tag:GetResources",
        "xray:GetTraceSummaries",
        "xray:BatchGetTraces"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "logs:FilterLogEvents",
        "logs:StartLiveTail",
        "logs:StopLiveTail"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/lambda/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSLambda_ReadOnlyAccess

Deskripsi: Memberikan akses hanya-baca ke layanan AWS Lambda, fitur konsol AWS Lambda, dan layanan terkait lainnya. AWS

`AWSLambda_ReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSLambda_ReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 17 November 2020, 21:10 UTC
- Waktu telah diedit: 17 Maret 2025, 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambda_ReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks",
        "cloudformation:ListStackResources",
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics",
        "ec2:DescribeSecurityGroups",
```

```
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "kms:ListAliases",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "logs:DescribeLogGroups",
        "lambda:Get*",
        "lambda:List*",
        "states:DescribeStateMachine",
        "states:ListStateMachines",
        "tag:GetResources",
        "xray:GetTraceSummaries",
        "xray:BatchGetTraces"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "logs:FilterLogEvents",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:DescribeQueries",
        "logs:GetLogGroupFields",
        "logs:GetLogRecord",
        "logs:GetQueryResults",
        "logs:StartLiveTail",
        "logs:StopLiveTail"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/lambda/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSLambdaBasicExecutionRole

Deskripsi: Memberikan izin menulis ke CloudWatch Log.

`AWSLambdaBasicExecutionRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSLambdaBasicExecutionRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 09 April 2015, 15:03 UTC
- Waktu telah diedit: 09 April 2015, 15:03 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSLambdaDynamoDBExecutionRole

Deskripsi: Menyediakan daftar dan akses baca ke aliran DynamoDB dan izin menulis ke log. CloudWatch

`AWSLambdaDynamoDBExecutionRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSLambdaDynamoDBExecutionRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 09 April 2015, 15:09 UTC
- Waktu telah diedit: 09 April 2015, 15:09 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaDynamoDBExecutionRole`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeStream",
        "dynamodb:GetRecords",
        "dynamodb:GetShardIterator",
        "dynamodb:ListStreams",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSLambdaENIManagementAccess

Deskripsi: Memberikan izin minimum untuk fungsi Lambda untuk ENIs mengelola (membuat, mendeskripsikan, menghapus) yang digunakan oleh Fungsi Lambda berkemampuan VPC.

`AWSLambdaENIManagementAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSLambdaENIManagementAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 06 Desember 2016 00:37 UTC
- Waktu yang telah diedit: 01 Oktober 2020, 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaENIManagementAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
```

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSLambdaExecute

Deskripsi: Menyediakan Put, Dapatkan akses ke S3 dan akses penuh ke CloudWatch Log.

`AWSLambdaExecute`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSLambdaExecute` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu telah diedit: 06 Februari 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambdaExecute`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:*"
      ],
      "Resource" : "arn:aws:logs:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSLambdaFullAccess

Deskripsi: Kebijakan ini berada di jalur penghentian. Lihat dokumentasi untuk panduan: https:// docs.aws.amazon.com/lambda/ latest/dg/access - control-identity-based .html. Menyediakan akses penuh ke Lambda, S3, DynamoDB, Metrik dan Log. CloudWatch

`AWSLambdaFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSLambdaFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu telah diedit: 27 November 2017, 23:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambdaFullAccess`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:GetTemplate",
        "cloudformation:ListStackResources",
        "cloudwatch:*",
        "cognito-identity:ListIdentityPools",
        "cognito-sync:GetCognitoEvents",
        "cognito-sync:SetCognitoEvents",
        "dynamodb:*",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
```

```
        "events:*",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:PassRole",
        "iot:AttachPrincipalPolicy",
        "iot:AttachThingPrincipal",
        "iot:CreateKeysAndCertificate",
        "iot:CreatePolicy",
        "iot:CreateThing",
        "iot:CreateTopicRule",
        "iot:DescribeEndpoint",
        "iot:GetTopicRule",
        "iot:ListPolicies",
        "iot:ListThings",
        "iot:ListTopicRules",
        "iot:ReplaceTopicRule",
        "kinesis:DescribeStream",
        "kinesis:ListStreams",
        "kinesis:PutRecord",
        "kms:ListAliases",
        "lambda:*",
        "logs:*",
        "s3:*",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "sns:Publish",
        "sns:Subscribe",
        "sns:Unsubscribe",
        "sqs:ListQueues",
        "sqs:SendMessage",
        "tag:GetResources",
        "xray:PutTelemetryRecords",
        "xray:PutTraceSegments"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSLambdaInvocation-DynamoDB

Deskripsi: Menyediakan akses baca ke DynamoDB Streams.

`AWSLambdaInvocation-DynamoDB`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSLambdaInvocation-DynamoDB` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu telah diedit: 06 Februari 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambdaInvocation-DynamoDB`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeStream",
        "dynamodb:GetRecords",
        "dynamodb:GetShardIterator",
        "dynamodb:ListStreams"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSLambdaKinesisExecutionRole

Deskripsi: Menyediakan daftar dan akses baca ke aliran Kinesis dan izin menulis ke log. CloudWatch

`AWSLambdaKinesisExecutionRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSLambdaKinesisExecutionRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 09 April 2015, 15:14 UTC
- Waktu telah diedit: 19 November 2018, 20:09 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaKinesisExecutionRole`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:DescribeStream",
        "kinesis:DescribeStreamSummary",
        "kinesis:GetRecords",
        "kinesis:GetShardIterator",
        "kinesis:ListShards",
        "kinesis:ListStreams",
        "kinesis:SubscribeToShard",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSLambdaMSKExecutionRole

Deskripsi: Memberikan izin yang diperlukan untuk mengakses MSK Cluster dalam VPC, mengelola ENIs (membuat, mendeskripsikan, menghapus) di VPC dan menulis izin ke Log. CloudWatch

`AWSLambdaMSKExecutionRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSLambdaMSKExecutionRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 11 Agustus 2020, 17:35 UTC
- Waktu yang telah diedit: 02 Agustus 2022, 20.08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaMSKExecutionRole`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kafka:DescribeCluster",
        "kafka:DescribeClusterV2",
        "kafka:GetBootstrapBrokers",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSLambdaReplicator

Deskripsi: Memberikan izin yang diperlukan Lambda Replicator untuk mereplikasi fungsi di seluruh wilayah

`AWSLambdaReplicator`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 23 Mei 2017, 17:53 UTC
- Waktu telah diedit: 08 Desember 2017, 00:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLambdaReplicator`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LambdaCreateDeletePermission",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:DisableReplication"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*"
      ]
    },
    {
```

```
      "Sid" : "IamPassRolePermission",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLikeIfExists" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudFrontListDistributions",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:ListDistributionsByLambdaFunction"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSLambdaRole

Deskripsi: Kebijakan default untuk peran layanan AWS Lambda.

`AWSLambdaRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSLambdaRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu telah diedit: 06 Februari 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaRole`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSLambdaSQSQueueExecutionRole

Deskripsi: Menyediakan pesan terima, menghapus pesan, dan membaca akses atribut ke antrian SQS, dan menulis izin untuk log. CloudWatch

`AWSLambdaSQSQueueExecutionRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSLambdaSQSQueueExecutionRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 14 Juni 2018, 21:50 UTC
- Waktu yang telah diedit: 14 Juni 2018, 21:50 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaSQSQueueExecutionRole`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
        "sqs:ReceiveMessage",
        "sqs:DeleteMessage",
        "sqs:GetQueueAttributes",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSLambdaVPCAccessExecutionRole

Deskripsi: Memberikan izin minimum untuk fungsi Lambda untuk dijalankan saat mengakses sumber daya dalam VPC - membuat, mendeskripsikan, menghapus antarmuka jaringan, dan menulis izin ke Log. CloudWatch

`AWSLambdaVPCAccessExecutionRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSLambdaVPCAccessExecutionRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 11 Februari 2016, 23:15 UTC
- Waktu telah diedit: 05 Januari 2024, 22:38 UTC

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

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSLambdaVPCAccessExecutionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DeleteNetworkInterface",
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSLicenseManagerConsumptionPolicy

Deskripsi: Memberikan izin untuk mengizinkan akses ke tindakan AWS License Manager API yang diperlukan untuk menggunakan lisensi yang pengguna memiliki hak.

`AWSLicenseManagerConsumptionPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSLicenseManagerConsumptionPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 11 Agustus 2021 23:18 UTC
- Waktu yang telah diedit: 11 Agustus 2021, 23:18 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLicenseManagerConsumptionPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "license-manager:CheckoutLicense",
      "license-manager:CheckInLicense",
      "license-manager:ExtendLicenseConsumption",
      "license-manager:GetLicense"
```

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy

Deskripsi: Memungkinkan Layanan Langganan Linux AWS License Manager mengelola sumber daya atas nama Anda.

`AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 20 Desember 2022, 18:54 UTC
- Waktu yang telah diedit: 08 Juli 2024, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeRegions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "OrganizationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:DescribeAccount",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:ListAccountsForParent",
        "organizations:ListRoots",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "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/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSLicenseManagerMasterAccountRolePolicy

Deskripsi: Kebijakan peran akun master layanan AWS License Manager

`AWSLicenseManagerMasterAccountRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 26 November 2018, 19:03 UTC
- Waktu yang telah diedit: 31 Mei 2022, 20.50 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerMasterAccountRolePolicy`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSLicenseManagerMemberAccountRolePolicy

Deskripsi: Kebijakan peran akun anggota layanan AWS License Manager

`AWSLicenseManagerMemberAccountRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 26 November 2018, 19:04 UTC
- Waktu yang telah diedit: 15 November 2019, 22:09 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerMemberAccountRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LicenseManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "license-manager:UpdateLicenseSpecificationsForResource",
        "license-manager:GetLicenseConfiguration"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SSMPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListInventoryEntries",
        "ssm:GetInventory",
        "ssm:CreateAssociation",
        "ssm:CreateResourceDataSync",
```

```
        "ssm:DeleteResourceDataSync",
        "ssm:ListResourceDataSync",
        "ssm:ListAssociations"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "RAMPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:AcceptResourceShareInvitation",
        "ram:GetResourceShareInvitations"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSLicenseManagerServiceRolePolicy

Deskripsi: Kebijakan peran default layanan AWS License Manager

`AWSLicenseManagerServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 26 November 2018, 19:02 UTC
- Waktu yang telah diedit: 30 Juli 2021, 01:43 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IAMPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/license-
management.marketplace.amazonaws.com/AWSServiceRoleForMarketplaceLicenseManagement"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "license-management.marketplace.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMPermissionsForCreatingMemberSLR",
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:*:iam::*:role/aws-service-role/license-manager.member-
account.amazonaws.com/AWSServiceRoleForAWSLicenseManagerMemberAccountRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "license-manager.member-account.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "S3BucketPermissions1",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-license-manager-service-*"
      ]
    },
    {
      "Sid" : "S3BucketPermissions2",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "S3ObjectPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-license-manager-service-*"
      ]
    },
```

```
    {
      "Sid" : "SNSAccountPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:aws-license-manager-service-*"
      ]
    },
    {
      "Sid" : "SNSTopicPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeImages",
        "ec2:DescribeHosts"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SSMPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListInventoryEntries",
        "ssm:GetInventory",
        "ssm:CreateAssociation"
      ],
      "Resource" : [
        "*"
      ]
    },
```

```
    {
      "Sid" : "OrganizationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "LicenseManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "license-manager:GetServiceSettings",
        "license-manager:GetLicense*",
        "license-manager:UpdateLicenseSpecificationsForResource",
        "license-manager:List*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSLicenseManagerUserSubscriptionsServiceRolePolicy

Deskripsi: Memungkinkan Layanan Langganan Pengguna AWS License Manager mengelola sumber daya atas nama Anda.

`AWSLicenseManagerUserSubscriptionsServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 30 Juli 2022, 01:17 UTC
- Waktu telah diedit: November 08, 2024, 02:54 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerUserSubscriptionsServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DSReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ds:DescribeDirectories",
        "ds:GetAuthorizedApplicationDetails"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMReadPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ssm:GetInventory",
        "ssm:GetCommandInvocation",
        "ssm:ListCommandInvocations",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeVpcPeeringConnections"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2WritePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances",
        "ec2:CreateTags"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:productCode" : [
            "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-*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSM2ServicePolicy

Deskripsi: Memungkinkan AWS M2 mengelola AWS sumber daya atas nama Anda.

`AWSM2ServicePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan

- Waktu pembuatan: 07 Juni 2022, 20:26 UTC
- Waktu yang telah diedit: 07 Juni 2022, 20.26 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSM2ServicePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeMountTargets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:DeregisterTargets"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeFileSystems"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/M2"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSManagedServices_ContactsServiceRolePolicy

Deskripsi: Memungkinkan AWS Managed Services membaca nilai tag pada AWS sumber daya

`AWSManagedServices_ContactsServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 23 Maret 2023, 17:07 UTC
- Waktu telah diedit: 23 Maret 2023, 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_ContactsServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy

Deskripsi: AWS Managed Services - kebijakan untuk mengelola infrastruktur kontrol detektif

`AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 19 Desember 2022, 23:11 UTC
- Waktu telah diedit: 19 Desember 2022, 23.11 UTC

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

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSManagedServices_EventsServiceRolePolicy

Deskripsi: Kebijakan AWS Managed Services untuk mengaktifkan fitur prosesor acara AMS.

`AWSManagedServices_EventsServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 07 Februari 2023, 18:41 UTC
- Waktu telah diedit: 07 Februari 2023, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_EventsServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:PutTargets",
        "events:PutRule",
        "events:RemoveTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "events.managedservices.amazonaws.com"
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSManagedServices_SelfServiceReporting_ServiceRolePolicy

Deskripsi: Memungkinkan fitur Pelaporan Layanan AWS Mandiri Layanan Terkelola Amazon untuk membaca data AWS Organisasi atas nama Anda guna mengaktifkan pelaporan agregat tingkat organisasi

`AWSManagedServices_SelfServiceReporting_ServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 08 Januari 2025, 21:22 UTC
- Waktu telah diedit: 08 Januari 2025, 21:22 UTC

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

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
        "organizations:DescribeAccount",
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSManagedServicesDeploymentToolkitPolicy

Deskripsi: Memungkinkan AWS Managed Services mengelola toolkit penerapan atas nama Anda.

`AWSManagedServicesDeploymentToolkitPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 09 Juni 2022, 18:33 UTC
- Waktu telah diedit: 04 April 2024, 20:41 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServicesDeploymentToolkitPolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSMarketplaceAmiIngestion

Deskripsi: Memungkinkan AWS Marketplace untuk menyalin Gambar Mesin Amazon Anda (AMIs) untuk mencantumkannya AWS Marketplace

`AWSMarketplaceAmiIngestion`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSMarketplaceAmiIngestion` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 25 September 2020, 20:55 UTC
- Waktu yang telah diedit: 25 September 2020, 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceAmiIngestion`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:ModifySnapshotAttribute"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:ec2:us-east-1::snapshot/snap-*"
    },
    {
      "Action" : [
        "ec2:DescribeImageAttribute",
        "ec2:DescribeImages",
        "ec2:DescribeSnapshotAttribute",
        "ec2:ModifyImageAttribute"
      ],
      "Effect" : "Allow",
```

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSMarketplaceDeploymentServiceRolePolicy

Deskripsi: Memungkinkan AWS Marketplace untuk membuat dan mengelola parameter penyebaran penjual untuk produk yang Anda berlangganan. AWS Marketplace

`AWSMarketplaceDeploymentServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 15 November 2023, 23:34 UTC
- Waktu telah diedit: 15 November 2023, 23:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceDeploymentServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ManageMarketplaceDeploymentSecrets",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:PutSecretValue",
        "secretsmanager:DescribeSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:RemoveRegionsFromReplication"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:marketplace-deployment*!*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ListSecrets",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:ListSecrets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "TagMarketplaceDeploymentSecrets",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource"
```

```
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:marketplace-deployment!*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/expirationDate" : "false"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "expirationDate"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSMarketplaceFullAccess

Deskripsi: Menyediakan kemampuan untuk berlangganan dan berhenti berlangganan AWS Marketplace perangkat lunak, memungkinkan pengguna untuk mengelola instans perangkat lunak Marketplace dari halaman 'Perangkat Lunak Anda' Marketplace, dan menyediakan akses administratif ke. EC2

`AWSMarketplaceFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSMarketplaceFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 11 Februari 2015, 17:21 UTC
- Waktu yang telah diedit: 07 Mei 2025, 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceFullAccess`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:*",
        "cloudformation:CreateStack",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:List*",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcs",
```

```
        "ec2:RunInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopyImage",
        "ec2:DeregisterImage",
        "ec2:DescribeSnapshots",
        "ec2:DeleteSnapshot",
        "ec2:CreateImage",
        "ec2:DescribeInstanceStatus",
        "ssm:GetAutomationExecution",
        "ssm:ListDocuments",
        "ssm:DescribeDocument",
        "sns:ListTopics",
        "sns:GetTopicAttributes",
        "sns:CreateTopic",
        "iam:GetRole",
        "iam:GetInstanceProfile",
        "iam:ListRoles",
        "iam:ListInstanceProfiles"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSMarketplaceGetEntitlements

Deskripsi: Menyediakan akses baca ke AWS Marketplace Hak

`AWSMarketplaceGetEntitlements`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSMarketplaceGetEntitlements` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Maret 2017, 19:37 UTC
- Waktu telah diedit: April 05, 2024, 01:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceGetEntitlements`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSMarketplaceGetEntitlements",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:GetEntitlements"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSMarketplaceImageBuildFullAccess

Deskripsi: Menyediakan akses penuh ke Fitur Pembuatan Gambar AWS Marketplace Pribadi. Selain membuat gambar pribadi, ia juga menyediakan izin untuk menambahkan tag ke gambar, meluncurkan dan menghentikan instance ec2.

`AWSMarketplaceImageBuildFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSMarketplaceImageBuildFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 31 Juli 2018, 23:29 UTC
- Waktu yang telah diedit: 04 Maret 2022, 17.05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceImageBuildFullAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListBuilds",
        "aws-marketplace:StartBuild",
        "aws-marketplace:DescribeBuilds"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:TerminateInstances",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/marketplace-image-build:build-id" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/*Automation*",
```

```
        "arn:aws:iam::*:role/*Instance*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution",
        "ssm:ListDocuments",
        "ssm:DescribeDocument",
        "ec2:DeregisterImage",
        "ec2:CopyImage",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeImages",
        "ec2:DescribeSubnets",
        "ec2:DeleteSnapshot",
        "ec2:CreateImage",
        "ec2:RunInstances",
        "ec2:DescribeInstanceStatus",
        "sns:GetTopicAttributes",
        "iam:GetRole",
        "iam:GetInstanceProfile"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::*image-build*"
      ]
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:*image-build*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:eu-central-1:906690553262:automation-definition/*",
        "arn:aws:ssm:us-east-1:058657716661:automation-definition/*",
        "arn:aws:ssm:ap-northeast-1:340648487307:automation-definition/*",
        "arn:aws:ssm:eu-west-1:564714592864:automation-definition/*",
        "arn:aws:ssm:us-west-2:243045473901:automation-definition/*",
        "arn:aws:ssm:ap-southeast-2:362149219987:automation-definition/*",
        "arn:aws:ssm:eu-west-2:587945719687:automation-definition/*",
        "arn:aws:ssm:us-east-2:134937423163:automation-definition/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
```

```
            "ssm.amazonaws.com"
          ],
          "iam:AssociatedResourceARN" : [
            "arn:aws:ssm:eu-central-1:906690553262:automation-definition/*",
            "arn:aws:ssm:us-east-1:058657716661:automation-definition/*",
            "arn:aws:ssm:ap-northeast-1:340648487307:automation-definition/*",
            "arn:aws:ssm:eu-west-1:564714592864:automation-definition/*",
            "arn:aws:ssm:us-west-2:243045473901:automation-definition/*",
            "arn:aws:ssm:ap-southeast-2:362149219987:automation-definition/*",
            "arn:aws:ssm:eu-west-2:587945719687:automation-definition/*",
            "arn:aws:ssm:us-east-2:134937423163:automation-definition/*"
          ]
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/marketplace-image-build:build-id" : "*"
        },
        "StringNotEquals" : {
          "ec2:CreateAction" : "RunInstances"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSMarketplaceLicenseManagementServiceRolePolicy

Deskripsi: Mengaktifkan akses ke Layanan AWS dan Sumber Daya yang digunakan atau dikelola oleh AWS Marketplace untuk manajemen lisensi.

`AWSMarketplaceLicenseManagementServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 03 Desember 2020, 08:33 UTC
- Waktu telah diedit: 03 Desember 2020, 08:33 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceLicenseManagementServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSMarketplaceManageSubscriptions

Deskripsi: Memberikan kemampuan untuk berlangganan dan berhenti berlangganan perangkat lunak AWS Marketplace

`AWSMarketplaceManageSubscriptions`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSMarketplaceManageSubscriptions` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu telah diedit: 20 November 2024, 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceManageSubscriptions`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "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"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws-marketplace:AgreementType" : [
            "PurchaseAgreement"
          ]
        },
        "Null" : {
          "aws-marketplace:AgreementType" : "false"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSMarketplaceMeteringFullAccess

Deskripsi: Menyediakan akses penuh ke AWS Marketplace Metering.

`AWSMarketplaceMeteringFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSMarketplaceMeteringFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 17 Maret 2016, 22:39 UTC
- Waktu telah diedit: 17 Maret 2016, 22:39 UTC

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

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSMarketplaceMeteringRegisterUsage

Deskripsi: Memberikan izin untuk mendaftarkan sumber daya dan melacak penggunaan melalui Layanan AWS Marketplace Pengukuran.

`AWSMarketplaceMeteringRegisterUsage`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSMarketplaceMeteringRegisterUsage` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 21 November 2019, 01:17 UTC
- Waktu yang telah diedit: 21 November 2019, 01:17 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceMeteringRegisterUsage`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSMarketplaceProcurementSystemAdminFullAccess

Deskripsi: Menyediakan akses penuh ke semua tindakan administratif untuk integrasi AWS Marketplace eProcurement.

`AWSMarketplaceProcurementSystemAdminFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSMarketplaceProcurementSystemAdminFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 25 Juni 2019, 13:07 UTC
- Waktu yang telah diedit: 25 Juni 2019, 13:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceProcurementSystemAdminFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      "Action" : [
        "aws-marketplace:PutProcurementSystemConfiguration",
        "aws-marketplace:DescribeProcurementSystemConfiguration",
        "organizations:Describe*",
        "organizations:List*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSMarketplacePurchaseOrdersServiceRolePolicy

Deskripsi: Memungkinkan akses untuk AWS Marketplace layanan untuk manajemen pesanan pembelian.

`AWSMarketplacePurchaseOrdersServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 27 Oktober 2021 15:12 UTC
- Waktu yang telah diedit: 27 Oktober 2021 15.12 UTC

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

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowPurchaseOrderActions",
      "Effect" : "Allow",
      "Action" : [
        "purchase-orders:ViewPurchaseOrders",
        "purchase-orders:ModifyPurchaseOrders"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSMarketplaceRead-only

Deskripsi: Memberikan kemampuan untuk meninjau AWS Marketplace langganan

`AWSMarketplaceRead-only`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSMarketplaceRead-only` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu yang telah diedit: 07 Mei 2025, 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceRead-only`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "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"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListPrivateListings"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSMarketplaceResaleAuthorizationServiceRolePolicy

Deskripsi: Mengaktifkan akses ke Layanan AWS dan Sumber Daya yang digunakan atau dikelola oleh AWS Marketplace untuk Otorisasi Penjualan Kembali.

`AWSMarketplaceResaleAuthorizationServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 05 Maret 2024, 18:47 UTC
- Waktu telah diedit: 05 Maret 2024, 18:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceResaleAuthorizationServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowResaleAuthorizationShareActionsRAMCreate",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : [
        "arn:aws:ram:*:*:*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "ram:RequestedResourceType" : "aws-marketplace:Entity"
        },
        "ArnLike" : {
          "ram:ResourceArn" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/
ResaleAuthorization/*"
        },
        "Null" : {
          "ram:Principal" : "true"
        }
      }
    },
    {
      "Sid" : "AllowResaleAuthorizationShareActionsRAMAssociate",
      "Effect" : "Allow",
      "Action" : [
        "ram:AssociateResourceShare"
      ],
      "Resource" : [
        "arn:aws:ram:*:*:*"
      ],
      "Condition" : {
        "Null" : {
          "ram:Principal" : "false"
        },
        "StringEquals" : {
          "ram:ResourceShareName" : "AWSMarketplaceResaleAuthorization"
        }
      }
    },
    {
      "Sid" : "AllowResaleAuthorizationShareActionsRAMAccept",
      "Effect" : "Allow",
      "Action" : [
        "ram:AcceptResourceShareInvitation"
      ],
      "Resource" : [
        "arn:aws:ram:*:*:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ram:ResourceShareName" : "AWSMarketplaceResaleAuthorization"
        }
      }
```

```
    },
    {
      "Sid" : "AllowResaleAuthorizationShareActionsRAMGet",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShareInvitations",
        "ram:GetResourceShareAssociations"
      ],
      "Resource" : [
        "arn:aws:ram:*:*:*"
      ]
    },
    {
      "Sid" : "AllowResaleAuthorizationShareActionsMarketplace",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:PutResourcePolicy",
        "aws-marketplace:GetResourcePolicy"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/ResaleAuthorization/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "ram.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowResaleAuthorizationShareActionsMarketplaceDescribe",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/ResaleAuthorization/*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSMarketplaceSellerFullAccess

Deskripsi: Menyediakan akses penuh ke semua operasi penjual di AWS Marketplace dan AWS layanan lainnya seperti manajemen AMI.

`AWSMarketplaceSellerFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSMarketplaceSellerFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 02 Juli 2019, 20:40 UTC
- Waktu telah diedit: 14 Januari 2025, 19:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceSellerFullAccess`

Versi kebijakan

Versi kebijakan: v16 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSMarketplaceSellerOfferManagement

Deskripsi: Menyediakan akses penjual ke aktivitas manajemen Penawaran dan Perjanjian.

`AWSMarketplaceSellerOfferManagement`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSMarketplaceSellerOfferManagement` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 19 November 2024, 00:41 UTC
- Waktu telah diedit: 19 November 2024, 00:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceSellerOfferManagement`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSMarketplaceSellerProductsFullAccess

Deskripsi: Menyediakan penjual akses penuh ke halaman Produk AWS Marketplace Manajemen dan AWS layanan lain seperti manajemen AMI.

`AWSMarketplaceSellerProductsFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSMarketplaceSellerProductsFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 02 Juli 2019, 21:06 UTC
- Waktu yang telah diedit: 10 Desember 2024, 19:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceSellerProductsFullAccess`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:StartChangeSet",
        "aws-marketplace:CancelChangeSet",
        "aws-marketplace:ListEntities",
        "aws-marketplace:DescribeEntity",
        "aws-marketplace:ListAssessments",
        "aws-marketplace:DescribeAssessment",
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots",
        "ec2:ModifyImageAttribute",
        "ec2:ModifySnapshotAttribute"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "assets.marketplace.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "vendor-insights:GetDataSource",
        "vendor-insights:ListDataSources",
```

```
        "vendor-insights:ListSecurityProfiles",
        "vendor-insights:GetSecurityProfile",
        "vendor-insights:GetSecurityProfileSnapshot",
        "vendor-insights:ListSecurityProfileSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:TagResource",
        "aws-marketplace:UntagResource",
        "aws-marketplace:ListTagsForResource"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:GetResourcePolicy",
        "aws-marketplace:PutResourcePolicy",
        "aws-marketplace:DeleteResourcePolicy"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSMarketplaceSellerProductsReadOnly

Deskripsi: Berikan penjual akses hanya-baca ke halaman Produk AWS Marketplace Manajemen.

`AWSMarketplaceSellerProductsReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSMarketplaceSellerProductsReadOnly` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 02 Juli 2019, 21:40 UTC
- Waktu yang telah diedit: 10 Desember 2024, 18:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceSellerProductsReadOnly`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSMediaConnectServicePolicy

Deskripsi: Kebijakan default yang memungkinkan akses ke Layanan AWS dan Sumber Daya yang digunakan atau dikelola oleh MediaConnect.

`AWSMediaConnectServicePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan

- Waktu pembuatan: 03 April 2023, 22:11 UTC
- Waktu telah diedit: 03 April 2023, 22:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMediaConnectServicePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:UpdateService",
        "ecs:DeleteService",
        "ecs:CreateService",
        "ecs:DescribeServices",
        "ecs:PutAttributes",
        "ecs:DeleteAttributes",
        "ecs:RunTask",
        "ecs:ListTasks",
        "ecs:StartTask",
        "ecs:StopTask",
        "ecs:DescribeTasks",
        "ecs:DescribeContainerInstances",
        "ecs:UpdateContainerInstancesState"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ecs:cluster" : "arn:aws:ecs:*:*:cluster/MediaConnectGateway"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:CreateCluster",
        "ecs:RegisterTaskDefinition"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:UpdateCluster",
        "ecs:UpdateClusterSettings",
        "ecs:ListAttributes",
        "ecs:DescribeClusters",
        "ecs:DeregisterContainerInstance",
        "ecs:ListContainerInstances"
      ],
      "Resource" : "arn:aws:ecs:*:*:cluster/MediaConnectGateway"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSMediaLiveAnywhereServiceRolePolicy

Deskripsi: Memungkinkan MediaLive Di Mana Saja untuk membuat dan mengelola AWS sumber daya atas nama Anda.

`AWSMediaLiveAnywhereServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 14 April 2025, 22:07 UTC
- Waktu yang telah diedit: 14 April 2025, 22:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMediaLiveAnywhereServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSMediaTailorServiceRolePolicy

Deskripsi: Aktifkan akses ke AWS Sumber Daya yang digunakan atau dikelola oleh MediaTailor

`AWSMediaTailorServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 17 September 2021 22:27 UTC
- Waktu yang telah diedit: 17 September 2021, 22:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMediaTailorServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "logs:PutLogEvents",
      "Resource" : "arn:aws:logs:*:*:log-group:MediaTailor/*:log-stream:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:MediaTailor/*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSMigrationHubDiscoveryAccess

Deskripsi: Kebijakan memungkinkan AWSMigration HubService untuk menelepon AWSApplication DiscoveryService atas nama pelanggan.

`AWSMigrationHubDiscoveryAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSMigrationHubDiscoveryAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 14 Agustus 2017, 13:30 UTC
- Waktu yang telah diedit: 06 Agustus 2020, 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMigrationHubDiscoveryAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "aws:migrationhub:source-id"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "dms:AddTagsToResource",
      "Resource" : [
        "arn:aws:dms:*:*:endpoint:*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "aws:migrationhub:source-id"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceAttribute"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSMigrationHubDMSAccess

Deskripsi: Kebijakan Layanan Migrasi Database untuk berperan dalam akun pelanggan untuk memanggil Migration Hub

`AWSMigrationHubDMSAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSMigrationHubDMSAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 14 Agustus 2017, 14:00 UTC
- Waktu yang telah diedit: 07 Oktober 2019, 17:51 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMigrationHubDMSAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
    {
      "Action" : [
        "mgh:AssociateCreatedArtifact",
        "mgh:DescribeMigrationTask",
        "mgh:DisassociateCreatedArtifact",
        "mgh:ImportMigrationTask",
        "mgh:ListCreatedArtifacts",
        "mgh:NotifyMigrationTaskState",
        "mgh:PutResourceAttributes",
        "mgh:NotifyApplicationState",
        "mgh:DescribeApplicationState",
        "mgh:AssociateDiscoveredResource",
        "mgh:DisassociateDiscoveredResource",
        "mgh:ListDiscoveredResources"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/DMS/*"
    },
    {
      "Action" : [
        "mgh:ListMigrationTasks",
        "mgh:GetHomeRegion"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSMigrationHubFullAccess

Deskripsi: Kebijakan terkelola untuk menyediakan akses pelanggan ke Layanan Hub Migrasi

`AWSMigrationHubFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSMigrationHubFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 14 Agustus 2017, 14:02 UTC
- Waktu yang telah diedit: 19 Juni 2019, 21:14 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubFullAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
continuousexport.discovery.amazonaws.com/
AWSServiceRoleForApplicationDiscoveryServiceContinuousExport*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "continuousexport.discovery.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
continuousexport.discovery.amazonaws.com/
AWSServiceRoleForApplicationDiscoveryServiceContinuousExport*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "migrationhub.amazonaws.com",
            "dmsintegration.migrationhub.amazonaws.com",
            "smsintegration.migrationhub.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSMigrationHubOrchestratorConsoleFullAccess

Deskripsi: Menyediakan akses terbatas ke AWS Migration Hub, AWS Application Discovery Service, Amazon Simple Storage Service, dan AWS Secrets Manager. Kebijakan ini juga memberikan akses penuh ke layanan AWS Migration Hub Orchestrator.

`AWSMigrationHubOrchestratorConsoleFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSMigrationHubOrchestratorConsoleFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 20 April 2022, 02:26 UTC
- Waktu telah diedit: 05 Desember 2023, 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubOrchestratorConsoleFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSMigrationHubOrchestratorInstanceRolePolicy

Deskripsi: Kebijakan ini perlu dilampirkan untuk instans migrasi SAP dan MGN agar layanan kami mengatur instance dengan mengunduh skrip dari S3 dan mengambil nilai rahasia di dalam instance. EC2

`AWSMigrationHubOrchestratorInstanceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSMigrationHubOrchestratorInstanceRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 20 April 2022, 02:43 UTC
- Waktu yang telah diedit: 20 April 2022, 02.43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubOrchestratorInstanceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      "Resource" : "arn:aws:secretsmanager:*:*:secret:migrationhub-orchestrator-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::migrationhub-orchestrator-*",
        "arn:aws:s3:::aws-migrationhub-orchestrator-*/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSMigrationHubOrchestratorPlugin

Deskripsi: Menyediakan akses terbatas ke Amazon Simple Storage Service, AWS Secrets Manager, dan tindakan terkait Plugin untuk AWS Migration Hub Orchestrator.

`AWSMigrationHubOrchestratorPlugin`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSMigrationHubOrchestratorPlugin` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 20 April 2022, 02:25 UTC
- Waktu yang telah diedit: 20 April 2022, 02.25 UTC

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

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutObject",
        "s3:GetObject",
        "s3:GetBucketAcl"
      ],
      "Resource" : "arn:aws:s3:::migrationhub-orchestrator-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "execute-api:Invoke",
        "execute-api:ManageConnections"
      ],
      "Resource" : [
        "arn:aws:execute-api:*:*:*/prod/*/put-log-data",
        "arn:aws:execute-api:*:*:*/prod/*/put-metric-data"
      ]
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "migrationhub-orchestrator:RegisterPlugin",
        "migrationhub-orchestrator:GetMessage",
        "migrationhub-orchestrator:SendMessage"
      ],
      "Resource" : "arn:aws:migrationhub-orchestrator:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:migrationhub-orchestrator-*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSMigrationHubOrchestratorServiceRolePolicy

Deskripsi: Menyediakan izin yang diperlukan untuk Migration Hub Orchestrator untuk memigrasi dan memodernisasi beban kerja lokal Anda

`AWSMigrationHubOrchestratorServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 20 April 2022, 02:24 UTC
- Waktu telah diedit: 04 Maret 2024, 18:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubOrchestratorServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ApplicationDiscoveryService",
      "Effect" : "Allow",
      "Action" : [
        "discovery:DescribeConfigurations",
        "discovery:ListConfigurations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LaunchWizard",
      "Effect" : "Allow",
      "Action" : [
        "launchwizard:ListProvisionedApps",
        "launchwizard:DescribeProvisionedApp",
        "launchwizard:ListDeployments",
        "launchwizard:GetDeployment"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "EC2instances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ec2MGNLaunchTemplate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "mgn.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ec2LaunchTemplates",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeLaunchTemplates"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "getHomeRegion",
      "Action" : [
        "mgh:GetHomeRegion"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "SSMcommand",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
```

```
        "ssm:GetCommandInvocation",
        "ssm:CancelCommand"
      ],
      "Resource" : [
        "arn:aws:ssm:*::document/AWS-RunRemoteScript",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:s3:::aws-migrationhub-orchestrator-*",
        "arn:aws:s3:::migrationhub-orchestrator-*"
      ]
    },
    {
      "Sid" : "SSM",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "s3GetObject",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::migrationhub-orchestrator-*",
        "arn:aws:s3:::migrationhub-orchestrator-*/*"
      ]
    },
    {
      "Sid" : "EventBridge",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:DescribeRule",
        "events:DeleteRule",
        "events:PutRule",
        "events:RemoveTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/MigrationHubOrchestratorManagedRule*"
    },
```

```
    {
      "Sid" : "MGN",
      "Effect" : "Allow",
      "Action" : [
        "mgn:GetReplicationConfiguration",
        "mgn:GetLaunchConfiguration",
        "mgn:StartCutover",
        "mgn:FinalizeCutover",
        "mgn:StartTest",
        "mgn:UpdateReplicationConfiguration",
        "mgn:DescribeSourceServers",
        "mgn:MarkAsArchived",
        "mgn:ChangeServerLifeCycleState"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ec2DescribeImportImage",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImportImageTasks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "s3ListBucket",
      "Effect" : "Allow",
      "Action" : "s3:ListBucket",
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringLike" : {
          "s3:prefix" : "migrationhub-orchestrator-vmie-*"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess

Deskripsi: Memberikan akses penuh ke Ruang Refactor Hub AWS Migration dan layanan AWS terkait lainnya kecuali Gateway AWS Transit dan grup EC2 keamanan yang tidak diperlukan saat menggunakan lingkungan tanpa jembatan jaringan. Kebijakan ini juga mengecualikan izin yang diperlukan untuk AWS Lambda dan AWS Resource Access Manager karena izin tersebut dapat dicakup berdasarkan tag.

`AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 April 2023, 20:09 UTC
- Waktu yang telah diedit: 11 April 2024, 18:16 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSMigrationHubRefactorSpaces-SSMAutomationPolicy

Deskripsi: Gunakan dalam peran layanan IAM yang diteruskan ke dokumen Otomasi SSM AWSRefactorSpaces-CreateResources untuk memberikan izin yang diperlukan untuk menjalankan otomatisasi. Kebijakan ini memberikan akses baca/tulis ke EC2 tag untuk melacak kemajuan otomatisasi. Ketika jembatan jaringan lingkungan Refactor Spaces diaktifkan, otomatisasi juga menambahkan grup keamanan lingkungan ke EC2 instance untuk mengizinkan lalu lintas dari layanan Refactor Spaces lain di lingkungan. Kebijakan ini juga memberikan akses ke parameter SSM tindakan pasca peluncuran Layanan Migrasi Aplikasi.

`AWSMigrationHubRefactorSpaces-SSMAutomationPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSMigrationHubRefactorSpaces-SSMAutomationPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 10 Agustus 2023, 15:08 UTC
- Waktu yang telah diedit: Agustus 10, 2023, 15:08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMigrationHubRefactorSpaces-SSMAutomationPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyInstanceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/refactor-spaces:ssm:optin" : "true"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyInstanceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/refactor-spaces:ssm:optin" : "true"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "refactor-spaces:ssm:environment-id"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:GetParameters",
      "Resource" : "arn:aws:ssm:*:*:parameter/ManagedByAWSApplicationMigrationService-
*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSMigrationHubRefactorSpacesFullAccess

Deskripsi: Memberikan akses penuh ke AWS MigrationHub Refactor Spaces, fitur konsol AWS MigrationHub Refactor Spaces, dan AWS layanan terkait lainnya kecuali izin yang diperlukan untuk Lambda dan AWS Resource AWS Access Manager karena dapat dicakup berdasarkan tag.

`AWSMigrationHubRefactorSpacesFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSMigrationHubRefactorSpacesFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 November 2021, 07:12 UTC
- Waktu yang telah diedit: 11 April 2024, 17:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubRefactorSpacesFullAccess`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "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"
```

```
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSMigrationHubRefactorSpacesServiceRolePolicy

Deskripsi: Menyediakan akses ke AWS Sumber Daya yang dikelola atau digunakan oleh AWS Migration Hub Refactor Spaces.

`AWSMigrationHubRefactorSpacesServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 29 November 2021, 06:50 UTC
- Waktu yang telah diedit: 20 Juli 2023, 15:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubRefactorSpacesServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeTargetGroups",
        "ram:GetResourceShareAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteTransitGatewayVpcAttachment",
        "ec2:CreateRoute",
        "ec2:DeleteRoute",
        "ec2:DeleteTags",
        "ram:DeleteResourceShare",
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:environment-id" : "false"
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:DeleteVpcEndpointServiceConfigurations",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:application-id" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:CreateLoadBalancerListeners",
        "elasticloadbalancing:CreateListener",
        "elasticloadbalancing:DeleteListener",
        "elasticloadbalancing:DeleteTargetGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/refactor-spaces:route-id" : [
            "*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:PUT",
        "apigateway:POST",
        "apigateway:GET",
        "apigateway:PATCH",
        "apigateway:DELETE"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/vpclinks/*",
```

```
        "arn:aws:apigateway:*::/tags",
        "arn:aws:apigateway:*::/tags/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:application-id" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "apigateway:GET",
      "Resource" : "arn:aws:apigateway:*::/vpclinks/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DeleteLoadBalancer",
      "Resource" : "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-
nlb-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:CreateListener"
      ],
      "Resource" : [
        "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-nlb-*",
        "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-nlb-*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:route-id" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DeleteListener",
      "Resource" : "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-nlb-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "elasticloadbalancing:DeleteTargetGroup",
        "elasticloadbalancing:RegisterTargets"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DeregisterTargets"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:route-id" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:CreateTargetGroup"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:route-id" : "false"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSMigrationHubSMSAccess

Deskripsi: Kebijakan Layanan Migrasi Server untuk berperan dalam akun pelanggan untuk memanggil Migration Hub

`AWSMigrationHubSMSAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSMigrationHubSMSAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 14 Agustus 2017, 13:57 UTC
- Waktu yang telah diedit: 07 Oktober 2019, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMigrationHubSMSAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
        "mgh:AssociateCreatedArtifact",
        "mgh:DescribeMigrationTask",
        "mgh:DisassociateCreatedArtifact",
        "mgh:ImportMigrationTask",
        "mgh:ListCreatedArtifacts",
        "mgh:NotifyMigrationTaskState",
        "mgh:PutResourceAttributes",
        "mgh:NotifyApplicationState",
        "mgh:DescribeApplicationState",
        "mgh:AssociateDiscoveredResource",
        "mgh:DisassociateDiscoveredResource",
        "mgh:ListDiscoveredResources"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/SMS/*"
    },
    {
      "Action" : [
        "mgh:ListMigrationTasks",
        "mgh:GetHomeRegion"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSMigrationHubStrategyCollector

Deskripsi: Memberikan izin untuk mengizinkan komunikasi dengan layanan Rekomendasi Strategi Hub AWS Migrasi, akses baca/tulis ke bucket S3 yang terkait dengan layanan, akses Amazon API Gateway untuk mengunggah log dan metrik, akses AWS Secrets AWS Manager untuk mengambil kredensi, dan layanan terkait apa pun.

`AWSMigrationHubStrategyCollector`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSMigrationHubStrategyCollector` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 19 Oktober 2021 20:15 UTC
- Waktu telah diedit: April 01, 2024, 16:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubStrategyCollector`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MHSRAllowS3Resources",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:GetBucketAcl",
        "s3:CreateBucket",
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketVersioning",
        "s3:PutLifecycleConfiguration",
        "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}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSMigrationHubStrategyConsoleFullAccess

Deskripsi: Memberikan akses penuh ke layanan Rekomendasi Strategi Hub AWS Migrasi dan akses ke AWS layanan terkait melalui. AWS Management Console

`AWSMigrationHubStrategyConsoleFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSMigrationHubStrategyConsoleFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 19 Oktober 2021 20:13 UTC
- Waktu yang telah diedit: 09 November 2022, 00:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubStrategyConsoleFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:CreateBucket",
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketPolicy",
        "s3:PutBucketVersioning",
        "s3:PutLifecycleConfiguration"
      ],
      "Resource" : "arn:aws:s3:::migrationhub-strategy-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "discovery:GetDiscoverySummary",
        "discovery:DescribeTags",
        "discovery:DescribeConfigurations",
        "discovery:ListConfigurations"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "iam:AWSServiceName" : "migrationhub-strategy.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/migrationhub-
strategy.amazonaws.com/AWSMigrationHubStrategyServiceRolePolicy*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSMigrationHubStrategyServiceRolePolicy

Deskripsi: Aktifkan akses ke AWS Sumber Daya yang digunakan atau dikelola oleh layanan Rekomendasi Strategi AWS Migration Hub.

`AWSMigrationHubStrategyServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 19 Oktober 2021, 20:02 UTC

- Waktu yang telah diedit: 19 Oktober 2021, 20:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubStrategyServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSMobileHub_FullAccess

Deskripsi: Kebijakan ini dapat dilampirkan ke Pengguna, Peran, atau Grup mana pun, untuk memberikan izin kepada pengguna untuk membuat, menghapus, dan memodifikasi proyek (dan AWS sumber daya terkait) di AWS Mobile Hub. Ini juga mencakup izin untuk membuat dan mengunduh contoh kode sumber aplikasi seluler untuk setiap proyek Mobile Hub.

`AWSMobileHub_FullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSMobileHub_FullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 05 Januari 2016, 19:56 UTC
- Waktu yang telah diedit: 19 Desember 2019, 23:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMobileHub_FullAccess`

Versi kebijakan

Versi kebijakan: v14 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET",
        "apigateway:POST",
        "cloudfront:GetDistribution",
        "devicefarm:CreateProject",
        "devicefarm:ListJobs",
        "devicefarm:ListRuns",
        "devicefarm:GetProject",
        "devicefarm:GetRun",
        "devicefarm:ListArtifacts",
        "devicefarm:ListProjects",
        "devicefarm:ScheduleRun",
        "dynamodb:DescribeTable",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "iam:ListSAMLProviders",
        "lambda:ListFunctions",
        "sns:ListTopics",
        "lex:GetIntent",
        "lex:GetIntents",
        "lex:GetSlotType",
        "lex:GetSlotTypes",
        "lex:GetBot",
        "lex:GetBots",
        "lex:GetBotAlias",
        "lex:GetBotAliases",
        "mobilehub:*"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::*/aws-my-sample-app*.zip"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::*-mobilehub-*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::*-mobilehub-*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSMobileHub_ReadOnly

Deskripsi: Kebijakan ini dapat dilampirkan ke Pengguna, Peran, atau Grup mana pun, untuk memberikan izin kepada pengguna untuk membuat daftar dan melihat proyek di AWS Mobile Hub. Ini juga mencakup izin untuk membuat dan mengunduh contoh kode sumber aplikasi seluler untuk setiap proyek Mobile Hub. Itu tidak memungkinkan pengguna untuk memodifikasi konfigurasi apa pun untuk proyek Mobile Hub apa pun.

`AWSMobileHub_ReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSMobileHub_ReadOnly` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 05 Januari 2016, 19:55 UTC
- Waktu telah diedit: 23 Juli 2018, 21:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMobileHub_ReadOnly`

Versi kebijakan

Versi kebijakan: v10 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeTable",
        "iam:ListSAMLProviders",
        "lambda:ListFunctions",
        "sns:ListTopics",
        "lex:GetIntent",
        "lex:GetIntents",
        "lex:GetSlotType",
        "lex:GetSlotTypes",
        "lex:GetBot",
        "lex:GetBots",
        "lex:GetBotAlias",
        "lex:GetBotAliases",
```

```
        "mobilehub:ExportProject",
        "mobilehub:GenerateProjectParameters",
        "mobilehub:GetProject",
        "mobilehub:SynchronizeProject",
        "mobilehub:GetProjectSnapshot",
        "mobilehub:ListProjectSnapshots",
        "mobilehub:ListAvailableConnectors",
        "mobilehub:ListAvailableFeatures",
        "mobilehub:ListAvailableRegions",
        "mobilehub:ListProjects",
        "mobilehub:ValidateProject",
        "mobilehub:VerifyServiceRole",
        "mobilehub:DescribeBundle",
        "mobilehub:ExportBundle",
        "mobilehub:ListBundles"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::*/aws-my-sample-app*.zip"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSMSKReplicatorExecutionRole

Deskripsi: Memberikan izin ke Amazon MSK Replicator untuk mereplikasi data antara MSK Cluster.

`AWSMSKReplicatorExecutionRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSMSKReplicatorExecutionRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 06 Desember 2023, 00:07 UTC
- Waktu yang telah diedit: 25 Maret 2024, 21:36 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMSKReplicatorExecutionRole`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ClusterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kafka-cluster:Connect",
        "kafka-cluster:DescribeCluster",
        "kafka-cluster:AlterCluster",
        "kafka-cluster:DescribeTopic",
        "kafka-cluster:CreateTopic",
        "kafka-cluster:AlterTopic",
        "kafka-cluster:WriteData",
        "kafka-cluster:ReadData",
        "kafka-cluster:AlterGroup",
        "kafka-cluster:DescribeGroup",
```

```
        "kafka-cluster:DescribeTopicDynamicConfiguration",
        "kafka-cluster:AlterTopicDynamicConfiguration",
        "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/*/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSNetworkFirewallFullAccess

Deskripsi: Memberikan akses penuh ke layanan AWS Network Firewall, termasuk izin untuk membuat, mengonfigurasi, mengelola, dan menghapus sumber daya firewall, kebijakan, dan grup aturan. Selain itu mencakup izin untuk memodifikasi titik akhir VPC, kebijakan bucket S3, konfigurasi Log CloudWatch , dan membuat peran terkait layanan untuk Network Firewall dan layanan pengiriman log

`AWSNetworkFirewallFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSNetworkFirewallFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 10 Juni 2025, 21:52 UTC
- Waktu yang telah diedit: 10 Juni 2025, 21:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSNetworkFirewallFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSNetworkFirewallReadOnlyAccess

Deskripsi: Menyediakan akses hanya-baca ke sumber daya AWS Network Firewall melalui, AWS Management Console CLI, dan. SDKs Kebijakan ini memungkinkan pengguna untuk melihat dan

memantau konfigurasi firewall, kebijakan, grup aturan, dan sumber daya terkait, tanpa kemampuan untuk membuat perubahan.

`AWSNetworkFirewallReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSNetworkFirewallReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 10 Juni 2025, 21:52 UTC
- Waktu yang telah diedit: 10 Juni 2025, 21:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSNetworkFirewallReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSNetworkFirewallServiceRolePolicy

Deskripsi: Izinkan AWSNetwork Firewall untuk membuat dan mengelola sumber daya yang diperlukan untuk Firewall Anda.

`AWSNetworkFirewallServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 17 November 2020, 17:17 UTC
- Waktu telah diedit: 30 Maret 2023, 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSNetworkFirewallServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : "acm:DescribeCertificate",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "resource-groups:ListGroupResources",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "tag:GetResources",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "resource-groups.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint",
          "aws:RequestTag/AWSNetworkFirewallManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSNetworkFirewallManaged" : "true"
        }
      }
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSNetworkManagerCloudWANServiceRolePolicy

Deskripsi: Memungkinkan NetworkManager untuk mengakses sumber daya yang terkait dengan Jaringan Inti

`AWSNetworkManagerCloudWANServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 12 Juli 2022, 12:17 UTC
- Waktu yang telah diedit: 12 Juli 2022, 12.17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSNetworkManagerCloudWANServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTransitGatewayRouteTableAnnouncement",
        "ec2:DeleteTransitGatewayRouteTableAnnouncement",
        "ec2:EnableTransitGatewayRouteTablePropagation",
        "ec2:DisableTransitGatewayRouteTablePropagation"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSNetworkManagerFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon NetworkManager melalui AWS Management Console.

`AWSNetworkManagerFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSNetworkManagerFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 Desember 2019, 17:37 UTC
- Waktu yang telah diedit: 03 Desember 2019, 17:37 UTC

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

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "networkmanager:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "networkmanager.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSNetworkManagerReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon NetworkManager melalui AWS Management Console.

`AWSNetworkManagerReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSNetworkManagerReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 Desember 2019, 17:35 UTC
- Waktu yang telah diedit: 03 Desember 2019, 17:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSNetworkManagerReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
        "networkmanager:Describe*",
        "networkmanager:Get*",
        "networkmanager:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSNetworkManagerServiceRolePolicy

Deskripsi: Memungkinkan NetworkManager untuk mengakses sumber daya yang terkait dengan Jaringan Global Anda

`AWSNetworkManagerServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 03 Desember 2019, 14:03 UTC
- Waktu yang telah diedit: 27 Juli 2022 19.41 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSNetworkManagerServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSObservabilityAdminServiceRolePolicy

Deskripsi: Menyediakan akses untuk mengelola AWS Config Configuration Recorder, mengelola AWS Config Configuration Aggregator, membuat AWS Config Service Linked Role untuk fungsi Configuration Recorder, mengkonsumsi data konfigurasi perekam, dan membaca AWS data Organizations untuk fitur organisasi.

`AWSObservabilityAdminServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 27 November 2024, 19:36 UTC
- Waktu telah diedit: 27 November 2024, 19:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSObservabilityAdminServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSOpsWorks_FullAccess

Deskripsi: Menyediakan akses penuh ke AWS OpsWorks.

`AWSOpsWorks_FullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSOpsWorks_FullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 22 Januari 2021 16:29 UTC
- Waktu yang telah diedit: 22 Januari 2021, 16:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOpsWorks_FullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancers",
        "iam:GetRolePolicy",
        "iam:ListInstanceProfiles",
        "iam:ListRoles",
        "iam:ListUsers",
        "opsworks:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "opsworks.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSOpsWorksCloudWatchLogs

Deskripsi: Mengaktifkan OpsWorks instance dengan CWLogs integrasi yang diaktifkan untuk mengirimkan log dan membuat grup log yang diperlukan

`AWSOpsWorksCloudWatchLogs`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSOpsWorksCloudWatchLogs` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 Maret 2017, 17:47 UTC
- Waktu telah diedit: 30 Maret 2017, 17:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOpsWorksCloudWatchLogs`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSOpsWorksCMInstanceProfileRole

Deskripsi: Menyediakan akses S3 untuk instans yang diluncurkan oleh OpsWorks CM.

`AWSOpsWorksCMInstanceProfileRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSOpsWorksCMInstanceProfileRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 24 November 2016, 09:48 UTC
- Waktu yang telah diedit: 23 April 2021 17.34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOpsWorksCMInstanceProfileRole`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListMultipartUploadParts",
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::aws-opsworks-cm-*",
      "Effect" : "Allow"
    },
    {
      "Action" : "acm:GetCertificate",
      "Resource" : "*",
      "Effect" : "Allow"
    },
    {
      "Action" : "secretsmanager:GetSecretValue",
      "Resource" : "arn:aws:secretsmanager:*:*:opsworks-cm!aws-opsworks-cm-secrets-*",
      "Effect" : "Allow"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSOpsWorksCMServiceRole

Deskripsi: Kebijakan Peran Layanan yang akan digunakan untuk Membuat server OpsWorks CM.

`AWSOpsWorksCMServiceRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSOpsWorksCMServiceRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 24 November 2016 09:49 UTC
- Waktu yang telah diedit: 23 April 2021, 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSOpsWorksCMServiceRole`

Versi kebijakan

Versi kebijakan: v14 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:s3:::aws-opsworks-cm-*"
      ],
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteObject",
        "s3:DeleteBucket",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutBucketPolicy",
        "s3:PutObject",
        "s3:GetBucketTagging",
        "s3:PutBucketTagging"
      ]
    },
    {
      "Effect" : "Allow",
      "Resource" : [
```

```
        "*"
      ],
      "Action" : [
        "tag:UntagResources",
        "tag:TagResources"
      ]
    },
    {
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ],
      "Action" : [
        "ssm:DescribeInstanceInformation",
        "ssm:GetCommandInvocation",
        "ssm:ListCommandInvocations",
        "ssm:ListCommands"
      ]
    },
    {
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "ssm:resourceTag/aws:cloudformation:stack-name" : "aws-opsworks-cm-*"
        }
      },
      "Action" : [
        "ssm:SendCommand"
      ]
    },
    {
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:ssm:*::document/*",
        "arn:aws:s3:::aws-opsworks-cm-*"
      ],
      "Action" : [
        "ssm:SendCommand"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ],
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AssociateAddress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateImage",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSnapshot",
        "ec2:CreateTags",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteSnapshot",
        "ec2:DeregisterImage",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DisassociateAddress",
        "ec2:ReleaseAddress",
        "ec2:RunInstances",
        "ec2:StopInstances"
      ]
    },
    {
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-name" : "aws-opsworks-cm-*"
        }
      },
      "Action" : [
        "ec2:TerminateInstances",
        "ec2:RebootInstances"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:opsworks-cm:*:*:server/*"
      ],
      "Action" : [
        "opsworks-cm:DeleteServer",
        "opsworks-cm:StartMaintenance"
      ]
    },
    {
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/aws-opsworks-cm-*"
      ],
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:UpdateStack"
      ]
    },
    {
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/aws-opsworks-cm-*",
        "arn:aws:iam::*:role/service-role/aws-opsworks-cm-*"
      ],
      "Action" : [
        "iam:PassRole"
      ]
    },
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "acm:DeleteCertificate",
        "acm:ImportCertificate"
      ]
    },
    {
      "Effect" : "Allow",
```

```
      "Resource" : "arn:aws:secretsmanager:*:*:opsworks-cm!aws-opsworks-cm-secrets-*",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:TagResource",
        "secretsmanager:UntagResource"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:DeleteTags",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:elastic-ip/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSOpsWorksInstanceRegistration

Deskripsi: Menyediakan akses untuk EC2 instans Amazon untuk mendaftar dengan AWS OpsWorks tumpukan.

`AWSOpsWorksInstanceRegistration`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSOpsWorksInstanceRegistration` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 Juni 2016, 14:23 UTC
- Waktu telah diedit: 03 Juni 2016, 14:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOpsWorksInstanceRegistration`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSOpsWorksRegisterCLI_EC2

Deskripsi: Kebijakan untuk mengaktifkan pendaftaran EC2 instans melalui CLI OpsWorks

`AWSOpsWorksRegisterCLI_EC2`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSOpsWorksRegisterCLI_EC2` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 Juni 2019, 15:56 UTC
- Waktu yang telah diedit: 18 Juni 2019, 15:56 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOpsWorksRegisterCLI_EC2`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
        "opsworks:CreateLayer",
        "opsworks:DeregisterInstance",
        "opsworks:DescribeInstances",
        "opsworks:DescribeStackProvisioningParameters",
        "opsworks:DescribeStacks",
        "opsworks:UnassignInstance"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSOpsWorksRegisterCLI_OnPremises

Deskripsi: Kebijakan untuk mengaktifkan pendaftaran instans Lokal melalui CLI OpsWorks

`AWSOpsWorksRegisterCLI_OnPremises`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSOpsWorksRegisterCLI_OnPremises` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 Juni 2019, 15:33 UTC
- Waktu yang telah diedit: 18 Juni 2019, 15:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOpsWorksRegisterCLI_OnPremises`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "opsworks:AssignInstance",
        "opsworks:CreateLayer",
        "opsworks:DeregisterInstance",
        "opsworks:DescribeInstances",
        "opsworks:DescribeStackProvisioningParameters",
        "opsworks:DescribeStacks",
        "opsworks:UnassignInstance"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances"
      ],
```

```
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateGroup",
        "iam:AddUserToGroup"
      ],
      "Resource" : [
        "arn:aws:iam::*:group/AWS/OpsWorks/OpsWorks-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateUser",
        "iam:CreateAccessKey"
      ],
      "Resource" : [
        "arn:aws:iam::*:user/AWS/OpsWorks/OpsWorks-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachUserPolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:user/AWS/OpsWorks/OpsWorks-*"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : "arn:aws:iam::aws:policy/AWSOpsWorksInstanceRegistration"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSOrganizationsFullAccess

Deskripsi: Menyediakan akses penuh ke AWS Organizations.

`AWSOrganizationsFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSOrganizationsFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 November 2018, 20:31 UTC
- Waktu telah diedit: 22 April 2025, 20:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOrganizationsFullAccess`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      "Sid" : "AWSOrganizationsFullAccess",
      "Effect" : "Allow",
      "Action" : "organizations:*",
      "Resource" : "*"
    },
    {
      "Sid" : "AWSOrganizationsFullAccessAccount",
      "Effect" : "Allow",
      "Action" : [
        "account:PutAlternateContact",
        "account:DeleteAlternateContact",
        "account:GetAlternateContact",
        "account:GetContactInformation",
        "account:PutContactInformation",
        "account:ListRegions",
        "account:EnableRegion",
        "account:DisableRegion",
        "account:PutAccountName",
        "account:GetAccountInformation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSOrganizationsFullAccessCreateSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "organizations.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSOrganizationsReadOnlyAccess

Deskripsi: Menyediakan akses read-only ke Organizations AWS .

`AWSOrganizationsReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSOrganizationsReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 November 2018, 20:32 UTC
- Waktu telah diedit: 07 Juni 2024, 21:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOrganizationsReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
    {
      "Sid" : "AWSOrganizationsReadOnlyAccount",
      "Effect" : "Allow",
      "Action" : [
        "account:GetAlternateContact",
        "account:GetContactInformation",
        "account:ListRegions",
        "account:GetRegionOptStatus",
        "account:GetPrimaryEmail"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSOrganizationsServiceTrustPolicy

Deskripsi: Kebijakan untuk memungkinkan AWS Organizations berbagi kepercayaan dengan orang lain yang disetujui Layanan AWS untuk tujuan menyederhanakan konfigurasi pelanggan.

`AWSOrganizationsServiceTrustPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 10 Oktober 2017, 23:04 UTC

- Waktu telah diedit: November 01, 2017, 06:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSOrganizationsServiceTrustPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM

- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSOutpostsAuthorizeServerPolicy

Deskripsi: Kebijakan ini memberikan izin yang memungkinkan Anda menginstal server Outpost di jaringan lokal.

`AWSOutpostsAuthorizeServerPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSOutpostsAuthorizeServerPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 04 Januari 2023, 19:23 UTC
- Waktu telah diedit: 04 Januari 2023, 19:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOutpostsAuthorizeServerPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSOutpostsServiceRolePolicy

Deskripsi: Kebijakan Peran Tertaut Layanan untuk mengaktifkan akses ke AWS sumber daya yang dikelola oleh AWS Outposts

`AWSOutpostsServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 09 November 2020, 22:55 UTC
- Waktu yang telah diedit: 17 April 2025, 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSOutpostsServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSPanoramaApplianceRolePolicy

Deskripsi: Memungkinkan perangkat lunak AWS IoT pada Alat Panorama untuk AWS mengunggah log ke Amazon. CloudWatch

`AWSPanoramaApplianceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSPanoramaApplianceRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 01 Desember 2020, 13:13 UTC
- Waktu yang telah diedit: 01 Desember 2020, 13:13 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaApplianceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PanoramaDeviceCreateLogStream",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
```

```
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/panorama_device*:log-stream:*"
    },
    {
      "Sid" : "PanoramaDeviceCreateLogGroup",
      "Effect" : "Allow",
      "Action" : "logs:CreateLogGroup",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/panorama_device*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSPanoramaApplianceServiceRolePolicy

Deskripsi: Memungkinkan Alat AWS Panorama untuk mengunggah log ke Amazon CloudWatch, dan untuk mendapatkan objek dari titik akses Amazon S3 yang dibuat untuk digunakan dengan Panorama. AWS

`AWSPanoramaApplianceServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSPanoramaApplianceServiceRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 20 Oktober 2021 12:14 UTC
- Waktu yang telah diedit: 10 Desember 2024, 20:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaApplianceServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PanoramaDeviceCreateLogStream",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/panorama_device*:log-stream:*",
        "arn:aws:logs:*:*:log-group:/aws/panorama/devices/*"
      ]
    },
    {
      "Sid" : "PanoramaDeviceCreateLogGroup",
      "Effect" : "Allow",
      "Action" : "logs:CreateLogGroup",
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/panorama_device*",
        "arn:aws:logs:*:*:log-group:/aws/panorama/devices/*"
      ]
    },
    {
      "Sid" : "PanoramaDevicePutMetric",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "PanoramaDeviceMetrics"
```

```
        }
      }
    },
    {
      "Sid" : "PanoramaDeviceS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket",
        "s3:GetObjectVersion"
      ],
      "Resource" : [
        "arn:aws:s3:::*-nodepackage-store-*",
        "arn:aws:s3:::*-application-payload-store-*",
        "arn:aws:s3:*:*:accesspoint/panorama*"
      ],
      "Condition" : {
        "ArnLike" : {
          "s3:DataAccessPointArn" : "arn:aws:s3:*:*:accesspoint/panorama*"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSPanoramaFullAccess

Deskripsi: Menyediakan akses penuh ke AWS Panorama

`AWSPanoramaFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSPanoramaFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Desember 2020, 13:12 UTC
- Waktu telah diedit: 10 Desember 2024, 20:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPanoramaFullAccess`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "panorama:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource" : "*",
      "Condition" : {
        "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"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSPanoramaGreengrassGroupRolePolicy

Deskripsi: Mengizinkan fungsi AWS Lambda pada Alat Panorama untuk mengelola sumber daya di AWS Panorama, mengunggah log dan metrik ke Amazon CloudWatch, dan mengelola objek dalam ember yang dibuat untuk digunakan dengan Panorama.

`AWSPanoramaGreengrassGroupRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSPanoramaGreengrassGroupRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 01 Desember 2020, 13:10 UTC
- Waktu yang telah diedit: 06 Januari 2021 19.30 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaGreengrassGroupRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PanoramaS3Access",
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucket*",
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*aws-panorama*"
      ]
    },
    {
      "Sid" : "PanoramaCLoudWatchPutDashboard",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutDashboard",
      "Resource" : [
        "arn:aws:cloudwatch::*:dashboard/panorama*"
      ]
    },
    {
      "Sid" : "PanoramaCloudWatchPutMetricData",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*"
    },
    {
      "Sid" : "PanoramaGreenGrassCloudWatchAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents",
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/greengrass/*"
    },
    {
      "Sid" : "PanoramaAccess",
      "Effect" : "Allow",
      "Action" : [
        "panorama:*"
      ],
      "Resource" : [
        "*"
```

```
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSPanoramaSageMakerRolePolicy

Deskripsi: Memungkinkan Amazon SageMaker mengelola objek dalam ember yang dibuat untuk digunakan dengan AWS Panorama.

`AWSPanoramaSageMakerRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSPanoramaSageMakerRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 01 Desember 2020, 13:13 UTC
- Waktu yang telah diedit: 01 Desember 2020, 13:13 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaSageMakerRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PanoramaSageMakerS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:GetBucket*"
      ],
      "Resource" : [
        "arn:aws:s3:::*aws-panorama*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSPanoramaServiceLinkedRolePolicy

Deskripsi: Memungkinkan AWS Panorama mengelola sumber daya di AWS IoT, Secrets AWS Manager, dan Panorama. AWS

`AWSPanoramaServiceLinkedRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 20 Oktober 2021 12:12 UTC
- Waktu yang telah diedit: 20 Oktober 2021, 12:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSPanoramaServiceLinkedRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PanoramaIoTThingAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateThing",
        "iot:DeleteThing",
        "iot:DeleteThingShadow",
        "iot:DescribeThing",
        "iot:GetThingShadow",
        "iot:UpdateThing",
        "iot:UpdateThingShadow"
      ],
      "Resource" : [
```

```
        "arn:aws:iot:*:*:thing/panorama*"
      ]
    },
    {
      "Sid" : "PanoramaIoTCertificateAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:AttachThingPrincipal",
        "iot:DetachThingPrincipal",
        "iot:UpdateCertificate",
        "iot:DeleteCertificate",
        "iot:AttachPrincipalPolicy",
        "iot:DetachPrincipalPolicy"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/panorama*",
        "arn:aws:iot:*:*:cert/*"
      ]
    },
    {
      "Sid" : "PanoramaIoTCreateCertificateAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateKeysAndCertificate"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "PanoramaIoTCreatePolicyAndVersionAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreatePolicy",
        "iot:CreatePolicyVersion",
        "iot:AttachPolicy"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:policy/panorama*"
      ]
    },
    {
      "Sid" : "PanoramaIoTJobAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "iot:DescribeJobExecution",
        "iot:CreateJob",
        "iot:DeleteJob"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:job/panorama*",
        "arn:aws:iot:*:*:thing/panorama*"
      ]
    },
    {
      "Sid" : "PanoramaIoTEndpointAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:DescribeEndpoint"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "PanoramaReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "panorama:Describe*",
        "panorama:List*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret",
        "secretsmanager:CreateSecret",
        "secretsmanager:ListSecretVersionIds",
        "secretsmanager:DeleteSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:panorama*",
        "arn:aws:secretsmanager:*:*:secret:Panorama*"
```

```
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSPanoramaServiceRolePolicy

Deskripsi: Memungkinkan AWS Panorama mengelola sumber daya di Amazon S3 AWS , IoT, AWS IoT, Lambda AWS , Amazon, dan Log Amazon SageMaker CloudWatch , serta meneruskan peran layanan AWS ke GreenGrass IoT, IoT, dan Amazon. AWS GreenGrass SageMaker

`AWSPanoramaServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSPanoramaServiceRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 01 Desember 2020, 13:14 UTC
- Waktu yang telah diedit: 01 Desember 2020, 13:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PanoramaIoTThingAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateThing",
        "iot:DeleteThing",
        "iot:DeleteThingShadow",
        "iot:DescribeThing",
        "iot:GetThingShadow",
        "iot:UpdateThing",
        "iot:UpdateThingShadow"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/panorama*"
      ]
    },
    {
      "Sid" : "PanoramaIoTCertificateAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:AttachThingPrincipal",
        "iot:DetachThingPrincipal",
        "iot:UpdateCertificate",
        "iot:DeleteCertificate",
        "iot:AttachPrincipalPolicy",
        "iot:DetachPrincipalPolicy"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/panorama*",
        "arn:aws:iot:*:*:cert/*"
      ]
    },
    {
      "Sid" : "PanoramaIoTCreateCertificateAndPolicyAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateKeysAndCertificate",
        "iot:CreatePolicy"
```

```
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "PanoramaIoTCreatePolicyVersionAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreatePolicyVersion"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:policy/panorama*"
      ]
    },
    {
      "Sid" : "PanoramaIoTJobAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:DescribeJobExecution",
        "iot:CreateJob",
        "iot:DeleteJob"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:job/panorama*",
        "arn:aws:iot:*:*:thing/panorama*"
      ]
    },
    {
      "Sid" : "PanoramaIoTEndpointAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:DescribeEndpoint"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "PanoramaAccess",
      "Effect" : "Allow",
      "Action" : [
        "panorama:Describe*",
        "panorama:List*",
```

```
        "panorama:Get*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "PanoramaS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:DeleteBucket",
        "s3:ListBucket",
        "s3:GetBucket*",
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::*aws-panorama*"
      ]
    },
    {
      "Sid" : "PanoramaIAMPassSageMakerRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSPanoramaSageMakerRole",
        "arn:aws:iam::*:role/service-role/AWSPanoramaSageMakerRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PanoramaIAMPassGreengrassRoleAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSPanoramaGreengrassGroupRole",
        "arn:aws:iam::*:role/service-role/AWSPanoramaGreengrassGroupRole",
        "arn:aws:iam::*:role/AWSPanoramaGreengrassRole",
        "arn:aws:iam::*:role/service-role/AWSPanoramaGreengrassRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "greengrass.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PanoramaIAMPassIoTRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSPanoramaApplianceRole",
        "arn:aws:iam::*:role/service-role/AWSPanoramaApplianceRole"
      ],
      "Condition" : {
        "StringEqualsIfExists" : {
          "iam:PassedToService" : "iot.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PanoramaGreenGrassAccess",
      "Effect" : "Allow",
      "Action" : [
        "greengrass:AssociateRoleToGroup",
        "greengrass:AssociateServiceRoleToAccount",
        "greengrass:CreateResourceDefinition",
        "greengrass:CreateResourceDefinitionVersion",
        "greengrass:CreateCoreDefinition",
        "greengrass:CreateCoreDefinitionVersion",
        "greengrass:CreateDeployment",
        "greengrass:CreateFunctionDefinition",
```

```
        "greengrass:CreateFunctionDefinitionVersion",
        "greengrass:CreateGroup",
        "greengrass:CreateGroupCertificateAuthority",
        "greengrass:CreateGroupVersion",
        "greengrass:CreateLoggerDefinition",
        "greengrass:CreateLoggerDefinitionVersion",
        "greengrass:CreateSubscriptionDefinition",
        "greengrass:CreateSubscriptionDefinitionVersion",
        "greengrass:DeleteCoreDefinition",
        "greengrass:DeleteFunctionDefinition",
        "greengrass:DeleteResourceDefinition",
        "greengrass:DeleteGroup",
        "greengrass:DeleteLoggerDefinition",
        "greengrass:DeleteSubscriptionDefinition",
        "greengrass:DisassociateRoleFromGroup",
        "greengrass:DisassociateServiceRoleFromAccount",
        "greengrass:GetAssociatedRole",
        "greengrass:GetConnectivityInfo",
        "greengrass:GetCoreDefinition",
        "greengrass:GetCoreDefinitionVersion",
        "greengrass:GetDeploymentStatus",
        "greengrass:GetDeviceDefinition",
        "greengrass:GetDeviceDefinitionVersion",
        "greengrass:GetFunctionDefinition",
        "greengrass:GetFunctionDefinitionVersion",
        "greengrass:GetGroup",
        "greengrass:GetGroupCertificateAuthority",
        "greengrass:GetGroupCertificateConfiguration",
        "greengrass:GetGroupVersion",
        "greengrass:GetLoggerDefinition",
        "greengrass:GetLoggerDefinitionVersion",
        "greengrass:GetResourceDefinition",
        "greengrass:GetServiceRoleForAccount",
        "greengrass:GetSubscriptionDefinition",
        "greengrass:GetSubscriptionDefinitionVersion",
        "greengrass:ListCoreDefinitionVersions",
        "greengrass:ListCoreDefinitions",
        "greengrass:ListDeployments",
        "greengrass:ListDeviceDefinitionVersions",
        "greengrass:ListDeviceDefinitions",
        "greengrass:ListFunctionDefinitionVersions",
        "greengrass:ListFunctionDefinitions",
        "greengrass:ListGroupCertificateAuthorities",
        "greengrass:ListGroupVersions",
```

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSPartnerCentralFullAccess

Deskripsi: Menyediakan akses penuh ke AWS Partner Central dan terkait Layanan AWS.

`AWSPartnerCentralFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSPartnerCentralFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 November 2024, 23:33 UTC
- Waktu yang telah diedit: 10 Desember 2024, 18:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerCentralFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "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" : "PassAWSPartnerCentralSnapshotJobRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "iam:PassedToService" : "resource-snapshot-job.partnercentral-
selling.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSPartnerCentralOpportunityManagement

Deskripsi: Menyediakan akses yang diperlukan untuk kegiatan manajemen peluang.

`AWSPartnerCentralOpportunityManagement`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSPartnerCentralOpportunityManagement` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 14 November 2024, 19:09 UTC
- Waktu telah diedit: 04 Desember 2024, 23:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerCentralOpportunityManagement`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "OpportunityManagement",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:AcceptEngagementInvitation",
        "partnercentral:AssignOpportunity",
        "partnercentral:AssociateOpportunity",
        "partnercentral:CreateEngagement",
        "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:ListResourceSnapshotJobs",
        "partnercentral:ListResourceSnapshots",
        "partnercentral:ListSolutions",
        "partnercentral:RejectEngagementInvitation",
        "partnercentral:StartEngagementByAcceptingInvitationTask",
        "partnercentral:StartEngagementFromOpportunityTask",
        "partnercentral:StartResourceSnapshotJob",
```

```
        "partnercentral:StopResourceSnapshotJob",
        "partnercentral:SubmitOpportunity",
        "partnercentral:UpdateOpportunity"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListingAWSMarketplaceEntities",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListEntities"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSMarketplaceOffersAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/Offer/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSPartnerCentralSandboxFullAccess

Deskripsi: Menyediakan akses yang diperlukan untuk pengujian pengembang di katalog Sandbox.

`AWSPartnerCentralSandboxFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSPartnerCentralSandboxFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 14 November 2024, 19:10 UTC
- Waktu yang telah diedit: 10 Desember 2024, 18:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerCentralSandboxFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSPartnerCentralSellingResourceSnapshotJobExecutionRolePolicy

Deskripsi: Menyediakan akses ke ResourceSnapshotJob untuk membaca sumber daya dan memotretnya dalam keterlibatan target.

`AWSPartnerCentralSellingResourceSnapshotJobExecutionRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSPartnerCentralSellingResourceSnapshotJobExecutionRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 10 Desember 2024, 18:21 UTC
- Waktu yang telah diedit: 10 Desember 2024, 18:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerCentralSellingResourceSnapshotJobExecutionRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSPartnerLedSupportReadOnlyAccess

Deskripsi: Kebijakan ini dapat digunakan untuk memberikan akses hanya-baca APIs yang dapat membaca metadata layanan untuk layanan di Anda. Akun AWS Anda dapat menggunakan kebijakan ini untuk memberi mitra Anda di Program Dukungan yang Dipimpin Mitra akses ke layanan yang ditentukan di bagian detail izin di bawah ini.

`AWSPartnerLedSupportReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSPartnerLedSupportReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 22 November 2024, 20:06 UTC
- Waktu telah diedit: 22 November 2024, 20:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerLedSupportReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "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"
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSPCSComputeNodePolicy

Deskripsi: Memberikan izin ke node komputasi AWS PCS untuk terhubung ke kluster AWS PCS.

`AWSPCSComputeNodePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSPCSComputeNodePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 23 Juni 2025, 18:07 UTC
- Waktu yang telah diedit: 23 Juni 2025, 18:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPCSComputeNodePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      "Effect" : "Allow",
      "Action" : [
        "pcs:RegisterComputeNodeGroupInstance"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSPCSServiceRolePolicy

Deskripsi: Memberikan izin kepada PCS untuk mengelola sumber daya atas nama Anda.

`AWSPCSServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 27 Agustus 2024, 16:01 UTC
- Waktu yang telah diedit: 27 Agustus 2024, 16:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSPCSServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSPriceListServiceFullAccess

Deskripsi: Menyediakan akses penuh ke Layanan Daftar AWS Harga.

`AWSPriceListServiceFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSPriceListServiceFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 22 November 2017, 00:36 UTC
- Waktu telah diedit: 02 Juli 2024, 13:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPriceListServiceFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      "Sid" : "AWSPriceListServiceFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "pricing:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin dengan hak istimewa paling sedikit

AWSPrivateCAAuditor

Deskripsi: Menyediakan akses auditor ke AWS Private Certificate Authority

`AWSPrivateCAAuditor`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSPrivateCAAuditor` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 14 Februari 2023, 18:33 UTC
- Waktu telah diedit: 14 Februari 2023, 18:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateCAAuditor`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:CreateCertificateAuthorityAuditReport",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:DescribeCertificateAuthorityAuditReport",
        "acm-pca:GetCertificateAuthorityCsr",
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:GetPolicy",
        "acm-pca:ListPermissions",
        "acm-pca:ListTags"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:ListCertificateAuthorities"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSPrivateCAConnectorForKubernetesPolicy

Deskripsi: Memberikan izin penting untuk Konektor CA AWS Pribadi untuk Kubernetes.

`AWSPrivateCAConnectorForKubernetesPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSPrivateCAConnectorForKubernetesPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 19 Mei 2025, 19:22 UTC
- Waktu yang telah diedit: 19 Mei 2025, 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateCAConnectorForKubernetesPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:GetCertificate",
        "acm-pca:IssueCertificate"
      ],
```

```
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSPrivateCAFullAccess

Deskripsi: Menyediakan akses penuh ke Otoritas Sertifikat AWS Pribadi

`AWSPrivateCAFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSPrivateCAFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 14 Februari 2023, 18:20 UTC
- Waktu telah diedit: 14 Februari 2023, 18:20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateCAFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSPrivateCAPrivilegedUser

Deskripsi: Menyediakan akses pengguna sertifikat istimewa ke Otoritas Sertifikat AWS Pribadi

`AWSPrivateCAPrivilegedUser`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSPrivateCAPrivilegedUser` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 14 Februari 2023, 18:26 UTC
- Waktu telah diedit: 22 Januari 2025, 21:07 UTC

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

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSPrivateCAReadOnly

Deskripsi: Menyediakan akses baca saja ke AWS Private Certificate Authority

`AWSPrivateCAReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSPrivateCAReadOnly` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 14 Februari 2023, 18:30 UTC
- Waktu yang telah diedit: 14 Februari 2023, 18:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateCAReadOnly`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "acm-pca:DescribeCertificateAuthority",
      "acm-pca:DescribeCertificateAuthorityAuditReport",
      "acm-pca:ListCertificateAuthorities",
      "acm-pca:GetCertificateAuthorityCsr",
      "acm-pca:GetCertificateAuthorityCertificate",
      "acm-pca:GetCertificate",
      "acm-pca:GetPolicy",
      "acm-pca:ListPermissions",
      "acm-pca:ListTags"
    ],
    "Resource" : "*"
  }
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSPrivateCAUser

Deskripsi: Menyediakan akses pengguna sertifikat ke Otoritas Sertifikat AWS Pribadi

`AWSPrivateCAUser`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSPrivateCAUser` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 14 Februari 2023, 18:16 UTC
- Waktu telah diedit: 22 Januari 2025, 21:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateCAUser`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSPrivateMarketplaceAdminFullAccess

Deskripsi: Menyediakan akses penuh ke semua tindakan administratif untuk Marketplace AWS Pribadi.

`AWSPrivateMarketplaceAdminFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSPrivateMarketplaceAdminFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 November 2018, 16:32 UTC
- Waktu yang telah diedit: 11 Juni 2025, 16:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateMarketplaceAdminFullAccess`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSPrivateMarketplaceRequests

Deskripsi: Menyediakan akses untuk membuat permintaan di Marketplace AWS Pribadi.

`AWSPrivateMarketplaceRequests`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSPrivateMarketplaceRequests` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 Oktober 2019 21:44 UTC
- Waktu yang telah diedit: 28 Oktober 2019, 21:44 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateMarketplaceRequests`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:CreatePrivateMarketplaceRequests",
        "aws-marketplace:ListPrivateMarketplaceRequests",
        "aws-marketplace:DescribePrivateMarketplaceRequests"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSPrivateNetworksServiceRolePolicy

Deskripsi: Memungkinkan Layanan Jaringan AWS Pribadi untuk mengelola sumber daya atas nama pelanggan.

`AWSPrivateNetworksServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 16 Desember 2021 23:17 UTC
- Waktu yang telah diedit: 16 Desember 2021, 23:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSPrivateNetworksServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Private5G"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSProtonCodeBuildProvisioningBasicAccess

Deskripsi: Izin CodeBuild perlu menjalankan build untuk Penyediaan AWS CodeBuild Proton.

`AWSProtonCodeBuildProvisioningBasicAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSProtonCodeBuildProvisioningBasicAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 09 November 2022, 21:04 UTC
- Waktu yang telah diedit: 09 November 2022, 21.04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSProtonCodeBuildProvisioningBasicAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/codebuild/AWSProton-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "proton:NotifyResourceDeploymentStatusChange",
      "Resource" : "arn:aws:proton:*:*:*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSProtonCodeBuildProvisioningServiceRolePolicy

Deskripsi: Memungkinkan AWS Proton mengelola penyediaan sumber daya Proton menggunakan CodeBuild dan layanan lainnya atas nama Anda. AWS

`AWSProtonCodeBuildProvisioningServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 09 November 2022, 21:32 UTC
- Waktu yang telah diedit: 17 Mei 2023, 16:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSProtonCodeBuildProvisioningServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSProtonDeveloperAccess

Deskripsi: Menyediakan akses ke AWS Proton APIs dan Konsol Manajemen, tetapi tidak mengizinkan administrasi templat atau lingkungan Proton.

`AWSProtonDeveloperAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSProtonDeveloperAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 17 Februari 2021, 19:02 UTC
- Waktu yang telah diedit: 06 Juni 2024, 18:26 UTC
- ARN: `arn:aws:iam::aws:policy/AWSProtonDeveloperAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSProtonFullAccess

Deskripsi: Menyediakan akses penuh ke AWS Proton APIs dan Konsol Manajemen. Selain izin ini, akses ke Amazon S3 juga diperlukan untuk mendaftarkan bundel templat dari bucket S3 Anda, serta akses ke Amazon IAM untuk membuat dan mengelola peran layanan untuk Proton.

`AWSProtonFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSProtonFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 17 Februari 2021, 19:07 UTC
- Waktu yang telah diedit: 06 Juni 2024, 18:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSProtonFullAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSProtonReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke AWS Proton APIs dan Konsol Manajemen.

`AWSProtonReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSProtonReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 17 Februari 2021, 19:09 UTC
- Waktu yang telah diedit: 18 November 2022, 18.28 UTC
- ARN: `arn:aws:iam::aws:policy/AWSProtonReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      "Effect" : "Allow",
      "Action" : [
        "codepipeline:ListPipelineExecutions",
        "codepipeline:ListPipelines",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:GetPipelineExecution",
        "proton:GetAccountRoles",
        "proton:GetAccountSettings",
        "proton:GetEnvironment",
        "proton:GetEnvironmentAccountConnection",
        "proton:GetEnvironmentTemplate",
        "proton:GetEnvironmentTemplateMajorVersion",
        "proton:GetEnvironmentTemplateMinorVersion",
        "proton:GetEnvironmentTemplateVersion",
        "proton:GetRepository",
        "proton:GetRepositorySyncStatus",
        "proton:GetResourcesSummary",
        "proton:GetService",
        "proton:GetServiceInstance",
        "proton:GetServiceTemplate",
        "proton:GetServiceTemplateMajorVersion",
        "proton:GetServiceTemplateMinorVersion",
        "proton:GetServiceTemplateVersion",
        "proton:GetTemplateSyncConfig",
        "proton:GetTemplateSyncStatus",
        "proton:ListEnvironmentAccountConnections",
        "proton:ListEnvironmentOutputs",
        "proton:ListEnvironmentProvisionedResources",
        "proton:ListEnvironments",
        "proton:ListEnvironmentTemplateMajorVersions",
        "proton:ListEnvironmentTemplateMinorVersions",
        "proton:ListEnvironmentTemplates",
        "proton:ListEnvironmentTemplateVersions",
        "proton:ListRepositories",
        "proton:ListRepositorySyncDefinitions",
        "proton:ListServiceInstanceOutputs",
        "proton:ListServiceInstanceProvisionedResources",
        "proton:ListServiceInstances",
        "proton:ListServicePipelineOutputs",
        "proton:ListServicePipelineProvisionedResources",
        "proton:ListServices",
        "proton:ListServiceTemplateMajorVersions",
        "proton:ListServiceTemplateMinorVersions",
```

```
        "proton:ListServiceTemplates",
        "proton:ListServiceTemplateVersions",
        "proton:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSProtonServiceGitSyncServiceRolePolicy

Deskripsi: Kebijakan yang memungkinkan AWS Proton menyinkronkan definisi layanan, lingkungan, dan komponen Anda dari repositori git Anda ke Proton. AWS

`AWSProtonServiceGitSyncServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 04 April 2023, 15:55 UTC
- Waktu yang telah diedit: 04 April 2023, 15:55 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSProtonServiceGitSyncServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ProtonServiceSync",
      "Effect" : "Allow",
      "Action" : [
        "proton:GetService",
        "proton:UpdateService",
        "proton:UpdateServicePipeline",
        "proton:GetServiceInstance",
        "proton:CreateServiceInstance",
        "proton:UpdateServiceInstance",
        "proton:ListServiceInstances",
        "proton:GetComponent",
        "proton:CreateComponent",
        "proton:ListComponents",
        "proton:UpdateComponent",
        "proton:GetEnvironment",
        "proton:CreateEnvironment",
        "proton:ListEnvironments",
        "proton:UpdateEnvironment"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSProtonSyncServiceRolePolicy

Deskripsi: Kebijakan yang memungkinkan AWS Proton menyinkronkan konten repositori git Anda ke Proton atau menyinkronkan konten Proton ke repositori git Anda.

`AWSProtonSyncServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 23 November 2021 21:14 UTC
- Waktu telah diedit: 05 Mei 2024, 01:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSProtonSyncServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      "Action" : [
        "proton:UpdateServiceTemplateVersion",
        "proton:UpdateServiceTemplate",
        "proton:UpdateEnvironmentTemplateVersion",
        "proton:UpdateEnvironmentTemplate",
        "proton:GetServiceTemplateVersion",
        "proton:GetServiceTemplate",
        "proton:GetEnvironmentTemplateVersion",
        "proton:GetEnvironmentTemplate",
        "proton:DeleteServiceTemplateVersion",
        "proton:DeleteEnvironmentTemplateVersion",
        "proton:CreateServiceTemplateVersion",
        "proton:CreateServiceTemplate",
        "proton:CreateEnvironmentTemplateVersion",
        "proton:CreateEnvironmentTemplate",
        "proton:ListEnvironmentTemplateVersions",
        "proton:ListServiceTemplateVersions",
        "proton:CreateEnvironmentTemplateMajorVersion",
        "proton:CreateServiceTemplateMajorVersion"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AccessGitRepos",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection",
        "codeconnections:UseConnection"
      ],
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSPurchaseOrdersServiceRolePolicy

Deskripsi: Memberikan izin untuk melihat dan memodifikasi pesanan pembelian di konsol penagihan

`AWSPurchaseOrdersServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSPurchaseOrdersServiceRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Mei 2020, 18:15 UTC
- Waktu yang telah diedit: 01 Desember 2024, 17:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPurchaseOrdersServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSQuickSetupCFGCPacksPermissionsBoundary

Deskripsi: CFGCPacks PermissionsBoundary Kebijakan AWSQuick Pengaturan menentukan daftar izin yang diizinkan dalam peran IAM yang dibuat oleh Penyiapan Cepat. Penyiapan Cepat menggunakan peran yang dibuat dengan kebijakan ini untuk menerapkan paket AWS kesesuaian Config.

`AWSQuickSetupCFGCPacksPermissionsBoundary`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuickSetupCFGCPacksPermissionsBoundary` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 26 Juni 2024, 09:52 UTC
- Waktu telah diedit: 26 Juni 2024, 09:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupCFGCPacksPermissionsBoundary`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSQuickSetupDeploymentRolePolicy

Deskripsi: Menyediakan izin untuk AWS Systems Manager Quick Setup untuk menerapkan beberapa jenis konfigurasi. Jenis konfigurasi ini membuat peran dan otomatisasi IAM yang mengonfigurasi layanan dan fitur Amazon Web Services yang sering digunakan dengan praktik terbaik yang direkomendasikan.

`AWSQuickSetupDeploymentRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuickSetupDeploymentRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 26 Juni 2024, 09:55 UTC
- Waktu yang telah diedit: 10 Juni 2025, 13:22 UTC

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

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "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"
      ]
    },
    {
      "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: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"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-*",
        "arn:aws:iam::*:role/AWSOperationsPack-*"
      ]
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSQuickSetupDevOpsGuruPermissionsBoundary

Deskripsi: AWSQuick SetupDevOpsGuruPermissionsBoundary Kebijakan menentukan daftar izin yang diizinkan dalam peran IAM yang dibuat oleh Penyiapan Cepat. Penyiapan Cepat menggunakan peran yang dibuat dengan kebijakan ini untuk mengaktifkan dan mengonfigurasi Amazon DevOps Guru. Kebijakan ini juga menyediakan izin untuk mengaktifkan Systems Manager Explorer.

`AWSQuickSetupDevOpsGuruPermissionsBoundary`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuickSetupDevOpsGuruPermissionsBoundary` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 26 Juni 2024, 09:44 UTC
- Waktu telah diedit: 26 Juni 2024, 09:44 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupDevOpsGuruPermissionsBoundary`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSQuickSetupDistributorPermissionsBoundary

Deskripsi: QuickSetup membuat peran IAM yang memungkinkannya mengonfigurasi fitur Distributor Systems Manager atas nama Anda, dan menggunakan kebijakan ini saat membuat peran tersebut untuk menentukan batas izin mereka.

`AWSQuickSetupDistributorPermissionsBoundary`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuickSetupDistributorPermissionsBoundary` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 26 Juni 2024, 09:50 UTC
- Waktu telah diedit: 26 Juni 2024, 09:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupDistributorPermissionsBoundary`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSQuickSetupEnableAREXExecutionPolicy

Deskripsi: Kebijakan ini memberikan izin yang memungkinkan Systems Manager menjalankan runbook AWSQuickSetupType-EnableAREX Otomasi, yang memungkinkan AWS Resource Explorer untuk digunakan dengan Systems Manager.

`AWSQuickSetupEnableAREXExecutionPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuickSetupEnableAREXExecutionPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 15 November 2024, 22:45 UTC
- Waktu telah diedit: 15 November 2024, 22:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupEnableAREXExecutionPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSQuickSetupEnableDHMCExecutionPolicy

Deskripsi: Kebijakan ini memberikan izin yang memungkinkan prinsipal menjalankan runbook AWSQuickSetupType-EnableDHMC Otomasi, yang mengaktifkan Konfigurasi Manajemen Host Default.

`AWSQuickSetupEnableDHMCExecutionPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuickSetupEnableDHMCExecutionPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 15 November 2024, 21:27 UTC
- Waktu yang telah diedit: 15 November 2024, 21:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupEnableDHMCExecutionPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSQuickSetupJITNADeploymentRolePolicy

Deskripsi: Kebijakan ini memungkinkan Quick Setup untuk menerapkan jenis konfigurasi yang diperlukan untuk mengatur akses just-in-time node.

`AWSQuickSetupJITNADeploymentRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuickSetupJITNADeploymentRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 17 April 2025, 09:07 UTC
- Waktu telah diedit: 17 April 2025, 09:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupJITNADeploymentRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSQuickSetupManagedInstanceProfileExecutionPolicy

Deskripsi: Kebijakan ini memberikan izin administratif yang memungkinkan Systems Manager membuat profil instans IAM default untuk kemampuan Penyiapan Cepat dan melampirkannya ke EC2 instans Amazon yang belum memiliki instance. profil terlampir.

`AWSQuickSetupManagedInstanceProfileExecutionPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuickSetupManagedInstanceProfileExecutionPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 15 November 2024, 21:51 UTC
- Waktu telah diedit: 15 November 2024, 21:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupManagedInstanceProfileExecutionPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSQuickSetupManageJITNAResourcesExecutionPolicy

Deskripsi: Kebijakan ini memberikan izin untuk mengaktifkan akses just-in-time node untuk Systems Manager.

`AWSQuickSetupManageJITNAResourcesExecutionPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuickSetupManageJITNAResourcesExecutionPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 17 April 2025, 21:37 UTC
- Waktu yang telah diedit: 23 April 2025, 15:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupManageJITNAResourcesExecutionPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSQuickSetupPatchPolicyBaselineAccess

Deskripsi: Menyediakan izin hanya-baca untuk mengakses garis dasar tambalan yang telah dikonfigurasi oleh administrator di saat ini Akun AWS atau organisasi menggunakan Pengaturan Cepat.

`AWSQuickSetupPatchPolicyBaselineAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuickSetupPatchPolicyBaselineAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 26 Juni 2024, 09:38 UTC
- Waktu telah diedit: 26 Juni 2024, 09:38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupPatchPolicyBaselineAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSQuickSetupPatchPolicyDeploymentRolePolicy

Deskripsi: Menyediakan izin yang memungkinkan Penyiapan Cepat untuk membuat sumber daya yang terkait dengan konfigurasi kebijakan tambalan.

`AWSQuickSetupPatchPolicyDeploymentRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuickSetupPatchPolicyDeploymentRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 26 Juni 2024, 09:57 UTC
- Waktu telah diedit: 26 Juni 2024, 09:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupPatchPolicyDeploymentRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSQuickSetupPatchPolicyPermissionsBoundary

Deskripsi: QuickSetup membuat peran IAM yang memungkinkannya mengonfigurasi fitur Systems Manager Patch Manager atas nama Anda, dan menggunakan kebijakan ini saat membuat peran tersebut untuk menentukan batas izinnya.

`AWSQuickSetupPatchPolicyPermissionsBoundary`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuickSetupPatchPolicyPermissionsBoundary` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 26 Juni 2024, 09:46 UTC
- Waktu telah diedit: 26 Juni 2024, 09:46 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupPatchPolicyPermissionsBoundary`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PatchingAutomationRoleGetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
```

```
        "arn:aws:iam::*:role/AWS-QuickSetup-AutomationRole-*"
      ]
    },
    {
      "Sid" : "PatchingAutomationRolePassPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-AutomationRole-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DefaultInstanceRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:UpdateRole",
        "iam:GetRole"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:PrincipalTag/QuickSetupManagerID" : "*"
        },
        "ArnLike" : {
          "aws:PrincipalArn" : "arn:aws:iam::*:role/AWS-QuickSetup-AutomationRole-*"
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup"
      ]
    },
    {
      "Sid" : "DefaultInstanceRolePassPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PoliciesAttachPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore",
            "arn:aws:iam::aws:policy/AWSQuickSetupPatchPolicyBaselineAccess"
          ]
        },
        "StringLike" : {
          "aws:PrincipalTag/QuickSetupManagerID" : "*"
        },
        "ArnLike" : {
          "aws:PrincipalArn" : "arn:aws:iam::*:role/AWS-QuickSetup-AutomationRole-*"
        }
      },
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Sid" : "CreateSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
```

```
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "InstanceRoleAddPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:AddRoleToInstanceProfile"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ManagedInstanceRoleUpdatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateManagedInstanceRole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile",
        "iam:GetRolePolicy",
        "iam:ListInstanceProfilesForRole",
        "iam:ListRoles"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "InstanceProfileCreatePermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:CreateInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/AmazonSSMRoleForInstancesQuickSetup"
      ]
    },
    {
      "Sid" : "InstanceProfileAssociationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateIamInstanceProfile"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "ec2:InstanceProfile" : "true"
        },
        "ArnLike" : {
          "ec2:NewInstanceProfile" : "arn:aws:iam::*:instance-profile/
AmazonSSMRoleForInstancesQuickSetup"
        }
      }
    },
    {
      "Sid" : "InstanceProfileDisassociationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DisassociateIamInstanceProfile"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ec2:InstanceProfile" : "arn:aws:iam::*:instance-profile/
AmazonSSMRoleForInstancesQuickSetup"
        }
      }
    },
    {
      "Sid" : "SSMAssociationsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAssociationExecutions",
        "ssm:UpdateAssociation",
```

```
        "ssm:DescribeAssociation"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSQuickSetup-*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*:*:association/*"
      ]
    },
    {
      "Sid" : "BaselineS3Permissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:Put*",
        "s3:Get*",
        "s3:List*",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:DeleteBucket"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : [
            "${aws:PrincipalAccount}"
          ]
        }
      },
      "Resource" : "arn:aws:s3:::aws-quicksetup-patchpolicy-*"
    },
    {
      "Sid" : "PatchingFunctionsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:baseline-overrides-*",
        "arn:aws:lambda:*:*:function:delete-name-tags-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : [
            "${aws:PrincipalAccount}"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "LoggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/lambda/baseline-overrides-*",
        "arn:aws:logs:*:*:log-group:/aws/lambda/delete-name-tags-*"
      ]
    },
    {
      "Sid" : "SSMTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource",
        "ssm:RemoveTagsFromResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:managed-instance/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "QSConfigName-*"
        }
      }
    },
    {
      "Sid" : "EC2TaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "QSConfigName-*"
        }
      }
    },
```

```
    {
      "Sid" : "RoleTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:TagRole",
        "iam:UntagRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "QSConfigId-*"
        }
      }
    },
    {
      "Sid" : "PatchingReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetPatchBaseline",
        "ssm:GetInventory",
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeAssociation",
        "ssm:GetAutomationExecution",
        "ssm:ListTagsForResource",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PatchingAutomationsStartPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-definition/AWS-EnableExplorer*",
        "arn:aws:ssm:*:*:automation-definition/AWS-RunPatchBaseline*",
        "arn:aws:ssm:*:*:automation-definition/AWS-AttachIAMToInstance*",
        "arn:aws:ssm:*:*:automation-definition/QuickSetup-*",
        "arn:aws:ssm:*:*:automation-definition/AWSQuickSetup-*"
      ]
    },
    {
```

```
      "Sid" : "ReadOnlyPermissionsForEnablingExplorer",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "config:DescribeConfigurationRecorders",
        "compute-optimizer:GetEnrollmentStatus",
        "support:DescribeTrustedAdvisorChecks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ExplorerServiceSettingsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/ssm-patchmanager",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/EC2",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ExplorerOnboarded",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/Association",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ComputeOptimizer",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ConfigCompliance",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/OpsData-TrustedAdvisor",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/SupportCenterCase"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSQuickSetupSchedulerPermissionsBoundary

Deskripsi: AWSQuick SetupSchedulerPermissionsBoundary Kebijakan menentukan daftar izin yang diizinkan dalam peran IAM yang dibuat oleh Penyiapan Cepat. Penyiapan Cepat menggunakan peran yang dibuat dengan kebijakan ini untuk mengaktifkan dan mengonfigurasi operasi terjadwal di EC2 instans Amazon dan sumber daya lainnya.

`AWSQuickSetupSchedulerPermissionsBoundary`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuickSetupSchedulerPermissionsBoundary` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 26 Juni 2024, 09:53 UTC
- Waktu telah diedit: 26 Juni 2024, 09:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupSchedulerPermissionsBoundary`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSQuickSetupSSMDeploymentRolePolicy

Deskripsi: Kebijakan ini memberikan izin administratif yang memungkinkan Penyiapan Cepat membuat sumber daya yang digunakan selama proses orientasi Systems Manager.

`AWSQuickSetupSSMDeploymentRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuickSetupSSMDeploymentRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 15 November 2024, 22:53 UTC
- Waktu yang telah diedit: 05 Mei 2025, 10:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupSSMDeploymentRolePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSQuickSetupSSMDeploymentS3BucketRolePolicy

Deskripsi: Kebijakan ini memberikan izin untuk mencantumkan semua bucket S3 di akun; dan untuk mengelola dan mengambil informasi tentang bucket tertentu di akun utama yang dikelola melalui templat. AWS CloudFormation

`AWSQuickSetupSSMDeploymentS3BucketRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuickSetupSSMDeploymentS3BucketRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 15 November 2024, 22:01 UTC
- Waktu telah diedit: 15 November 2024, 22:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupSSMDeploymentS3BucketRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSQuickSetupSSMHostMgmtPermissionsBoundary

Deskripsi: Pengaturan Cepat membuat peran IAM yang memungkinkannya mengonfigurasi tipe Pengaturan Cepat Manajer Host atas nama Anda, dan menggunakan kebijakan ini saat membuat peran tersebut untuk menentukan batas izinnya.

`AWSQuickSetupSSMHostMgmtPermissionsBoundary`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuickSetupSSMHostMgmtPermissionsBoundary` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 26 Juni 2024, 09:48 UTC
- Waktu telah diedit: 26 Juni 2024, 09:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupSSMHostMgmtPermissionsBoundary`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSQuickSetupSSMLifecycleManagementExecutionPolicy

Deskripsi: Kebijakan ini memberikan izin administratif yang memungkinkan Penyiapan Cepat menjalankan sumber daya AWS CloudFormation khusus pada peristiwa siklus hidup selama penerapan Quick Setup di Systems Manager.

`AWSQuickSetupSSMLifecycleManagementExecutionPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuickSetupSSMLifecycleManagementExecutionPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 15 November 2024, 21:55 UTC
- Waktu telah diedit: 15 November 2024, 21:55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupSSMLifecycleManagementExecutionPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "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:*:*:automation-execution/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/QuickSetupDocument" : "AWSQuickSetupType-SSM",
          "aws:ResourceTag/QuickSetupDocument" : "AWSQuickSetupType-SSM"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSQuickSetupSSMManageResourcesExecutionPolicy

Deskripsi: Kebijakan ini memberikan izin yang memungkinkan Systems Manager membuat prasyarat seperti peran IAM yang diperlukan untuk orientasi Systems Manager.

`AWSQuickSetupSSMManageResourcesExecutionPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuickSetupSSMManageResourcesExecutionPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 15 November 2024, 22:49 UTC
- Waktu telah diedit: 15 November 2024, 22:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupSSMManageResourcesExecutionPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSQuickSightAssetBundleExportPolicy

Deskripsi: Menyediakan set izin yang diperlukan untuk melakukan Operasi Ekspor Bundel QuickSight Aset

`AWSQuickSightAssetBundleExportPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuickSightAssetBundleExportPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 27 Maret 2024, 21:31 UTC
- Waktu telah diedit: 27 Maret 2024, 21:31 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSightAssetBundleExportPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSQuickSightAssetBundleImportPolicy

Deskripsi: Menyediakan set izin yang diperlukan untuk melakukan Operasi Impor Bundel QuickSight Aset

`AWSQuickSightAssetBundleImportPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuickSightAssetBundleImportPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 27 Maret 2024, 21:40 UTC
- Waktu telah diedit: 27 Maret 2024, 21:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSightAssetBundleImportPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSQuicksightAthenaAccess

Deskripsi: Akses Quicksight ke Athena API dan bucket S3 yang digunakan untuk hasil kueri Athena

`AWSQuicksightAthenaAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuicksightAthenaAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 09 Desember 2016, 02:31 UTC
- Waktu yang telah diedit: 03 Januari 2025, 00:22 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuicksightAthenaAccess`

Versi kebijakan

Versi kebijakan: v11 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "athena:BatchGetQueryExecution",
        "athena:CancelQueryExecution",
        "athena:GetCatalogs",
        "athena:GetExecutionEngine",
        "athena:GetExecutionEngines",
        "athena:GetNamespace",
        "athena:GetNamespaces",
        "athena:GetQueryExecution",
        "athena:GetQueryExecutions",
        "athena:GetQueryResults",
        "athena:GetQueryResultsStream",
        "athena:GetTable",
        "athena:GetTables",
        "athena:ListQueryExecutions",
        "athena:RunQuery",
        "athena:StartQueryExecution",
        "athena:StopQueryExecution",
        "athena:ListWorkGroups",
        "athena:ListEngineVersions",
        "athena:GetWorkGroup",
        "athena:GetDataCatalog",
        "athena:GetDatabase",
        "athena:GetTableMetadata",
        "athena:ListDataCatalogs",
        "athena:ListDatabases",
        "athena:ListTableMetadata"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
```

```
        "glue:DeleteDatabase",
        "glue: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" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSQuickSightDescribeRDS

Deskripsi: Izinkan QuickSight untuk menggambarkan sumber daya RDS

`AWSQuickSightDescribeRDS`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuickSightDescribeRDS` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 10 November 2015, 23:24 UTC
- Waktu telah diedit: 10 November 2015, 23:24 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightDescribeRDS`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSQuickSightDescribeRedshift

Deskripsi: Izinkan QuickSight untuk menggambarkan sumber daya Redshift

`AWSQuickSightDescribeRedshift`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuickSightDescribeRedshift` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 10 November 2015, 23:25 UTC
- Waktu telah diedit: 10 November 2015, 23:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightDescribeRedshift`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSQuickSightElasticsearchPolicy

Deskripsi: Menyediakan akses ke sumber daya Amazon Elasticsearch dari Amazon QuickSight

`AWSQuickSightElasticsearchPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuickSightElasticsearchPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 09 September 2020, 17:27 UTC
- Waktu yang telah diedit: 07 September 2021, 23:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightElasticsearchPolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      "Resource" : [
        "arn:aws:es:*:*:domain/*/",
        "arn:aws:es:*:*:domain/*/_cluster/settings",
        "arn:aws:es:*:*:domain/*/_cat/indices"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "es:ListDomainNames",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "es:DescribeElasticsearchDomain",
        "es:DescribeDomain"
      ],
      "Resource" : [
        "arn:aws:es:*:*:domain/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "es:ESHttpPost",
        "es:ESHttpGet"
      ],
      "Resource" : [
        "arn:aws:es:*:*:domain/*/_opendistro/_sql",
        "arn:aws:es:*:*:domain/*/_plugin/_sql"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSQuickSightIoTAnalyticsAccess

Deskripsi: Berikan akses QuickSight hanya-baca ke kumpulan data IoT Analytics

`AWSQuickSightIoTAnalyticsAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuickSightIoTAnalyticsAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 November 2017, 17:00 UTC
- Waktu telah diedit: 29 November 2017, 17:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSightIoTAnalyticsAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "iotanalytics:ListDatasets",
        "iotanalytics:DescribeDataset",
        "iotanalytics:GetDatasetContent"
      ],
      "Effect" : "Allow",
```

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSQuickSightListIAM

Deskripsi: QuickSight Izinkan daftar entitas IAM

`AWSQuickSightListIAM`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuickSightListIAM` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 10 November 2015, 23:25 UTC
- Waktu telah diedit: 10 November 2015, 23:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightListIAM`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSQuicksightOpenSearchPolicy

Deskripsi: Menyediakan akses ke OpenSearch sumber daya Amazon dari Amazon QuickSight

`AWSQuicksightOpenSearchPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuicksightOpenSearchPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 07 September 2021 23:26 UTC

- Waktu yang telah diedit: 07 September 2021, 23:26 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuicksightOpenSearchPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "es:ESHttpGet"
      ],
      "Resource" : [
        "arn:aws:es:*:*:domain/*/",
        "arn:aws:es:*:*:domain/*/_cluster/settings",
        "arn:aws:es:*:*:domain/*/_cat/indices"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "es:ListDomainNames",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "es:DescribeDomain"
      ],
      "Resource" : [
        "arn:aws:es:*:*:domain/*"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "es:ESHttpPost",
        "es:ESHttpGet"
      ],
      "Resource" : [
        "arn:aws:es:*:*:domain/*/_opendistro/_sql",
        "arn:aws:es:*:*:domain/*/_plugin/_sql"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSQuickSightSageMakerPolicy

Deskripsi: Menyediakan akses ke SageMaker sumber daya Amazon dari Amazon QuickSight

`AWSQuickSightSageMakerPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuickSightSageMakerPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 17 Januari 2020, 17:18 UTC
- Waktu yang telah diedit: 30 Oktober 2023, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightSageMakerPolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SageMakerTransformJobAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeTransformJob",
        "sagemaker:StopTransformJob",
        "sagemaker:CreateTransformJob"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:transform-job/quicksight-auto-generated-*"
    },
    {
      "Sid" : "SageMakerModelReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker: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*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSQuickSightSecretsManagerWriteAccess

Deskripsi: Kebijakan yang digunakan oleh QuickSight untuk membuat AWS rahasia di Secrets Manager dan melampirkan kebijakan sumber daya pada QuickSight rahasia yang ada.

`AWSQuickSightSecretsManagerWriteAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuickSightSecretsManagerWriteAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan

- Waktu pembuatan: 22 Mei 2025, 01:22 UTC
- Waktu telah diedit: 22 Mei 2025, 01:22 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightSecretsManagerWriteAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSQuickSightSecretsManagerWritePolicy

Deskripsi: Kebijakan yang digunakan oleh QuickSight untuk membuat AWS rahasia di Secrets Manager dan melampirkan kebijakan sumber daya pada QuickSight rahasia yang ada.

`AWSQuickSightSecretsManagerWritePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuickSightSecretsManagerWritePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 12 Mei 2025, 19:22 UTC
- Waktu yang telah diedit: 12 Mei 2025, 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSightSecretsManagerWritePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSQuickSightTimestreamPolicy

Deskripsi: AWS QuickSight akses ke AWS Timestream APIs. Pelanggan dapat melampirkan kebijakan ini ke AWS QuickSight peran untuk memungkinkan pengambilan data dan metadata.

`AWSQuickSightTimestreamPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuickSightTimestreamPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 30 September 2020, 21:47 UTC
- Waktu yang telah diedit: 30 September 2020, 21:47 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightTimestreamPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "timestream:Select",
        "timestream:CancelQuery",
        "timestream:ListTables",
        "timestream:ListDatabases",
        "timestream:ListMeasures",
        "timestream:DescribeTable",
        "timestream:DescribeDatabase",
        "timestream:SelectValues",
        "timestream:DescribeEndpoints"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSReachabilityAnalyzerServiceRolePolicy

Deskripsi: Memungkinkan VPC Reachability Analyzer AWS mengakses sumber daya dan berintegrasi dengan Organizations atas nama Anda. AWS

`AWSReachabilityAnalyzerServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 23 November 2022, 17:12 UTC
- Waktu yang telah diedit: September 10, 2024, 16:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSReachabilityAnalyzerServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSRefactoringToolkitFullAccess

Deskripsi: Kebijakan ini memberikan izin untuk menggunakan AWS layanan dengan ekstensi AWS Toolkit for .NET Refactoring untuk Microsoft Visual Studio. Ini dimaksudkan untuk dilampirkan ke AWS profil lokal. Kebijakan ini memungkinkan mengunggah artefak aplikasi dan mengunduh artefak yang dihasilkan dari Amazon S3. Ini memungkinkan membangun aplikasi ke dalam gambar kontainer menggunakan AWS CodeBuild dan menyimpan dan mengambil gambar dari Amazon Elastic Container Registry (Amazon ECR). Dan itu memungkinkan penyebaran aplikasi ke layanan kontainer AWS seperti Amazon Elastic Container Service (Amazon ECS), pembuatan sumber daya VPC opsional, koneksi opsional ke infrastruktur yang ada seperti AWS Directory Service, dan layanan terkait lainnya.

`AWSRefactoringToolkitFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSRefactoringToolkitFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 25 Oktober 2022, 16:41 UTC
- Waktu telah diedit: 09 April 2025, 20:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRefactoringToolkitFullAccess`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSRefactoringToolkitSidecarPolicy

Deskripsi: Kebijakan ini dimaksudkan untuk digunakan oleh Amazon ECS Tasks yang dibuat untuk menguji aplikasi AWS menggunakan ekstensi AWS Toolkit for .NET Refactoring untuk Microsoft Visual Studio. Kebijakan ini memberikan akses untuk mengunduh artefak aplikasi dari Amazon S3, mengkomunikasikan status Tugas menggunakan Systems AWS Manager, dan layanan lain yang diperlukan.

`AWSRefactoringToolkitSidecarPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSRefactoringToolkitSidecarPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 25 Oktober 2022, 16:41 UTC
- Waktu yang telah diedit: 29 Oktober 2022, 22.15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRefactoringToolkitSidecarPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SsmMessagesAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:OpenControlChannel",
        "ssmmessages:CreateControlChannel",
        "ssmmessages:OpenDataChannel",
        "ssmmessages:CreateDataChannel"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3GetObjectAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::*/refactoringtoolkit*"
    },
    {
      "Sid" : "S3ListBucketAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringLike" : {
          "s3:prefix" : "refactoringtoolkit*"
        }
      }
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSrePostPrivateCloudWatchAccess

Deskripsi: Menyediakan akses Re:Post Private untuk mempublikasikan data metrik CloudWatch

`AWSrePostPrivateCloudWatchAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 15 November 2023, 16:37 UTC
- Waktu telah diedit: 15 November 2023, 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSrePostPrivateCloudWatchAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSRepostSpaceSupportOperationsPolicy

Deskripsi: Kebijakan ini memungkinkan layanan re:Post Space untuk membuat, mengelola, dan menyelesaikan kasus Support yang dibuat melalui aplikasi Space.

`AWSRepostSpaceSupportOperationsPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSRepostSpaceSupportOperationsPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 26 November 2023, 21:52 UTC
- Waktu telah diedit: 26 November 2023, 21:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRepostSpaceSupportOperationsPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RepostSpaceSupportOperations",
      "Effect" : "Allow",
      "Action" : [
        "support:AddAttachmentsToSet",
        "support:AddCommunicationToCase",
        "support:CreateCase",
        "support:DescribeCases",
        "support:DescribeCommunications",
        "support:ResolveCase"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSResilienceHubAsssessmentExecutionPolicy

Deskripsi: Kebijakan untuk peran layanan AWS Resilience Hub yang memungkinkan akses ke AWS layanan lain untuk melaksanakan penilaian.

`AWSResilienceHubAsssessmentExecutionPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSResilienceHubAsssessmentExecutionPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Juni 2023, 12:32 UTC
- Waktu yang telah diedit: 16 Desember 2024, 14:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResilienceHubAsssessmentExecutionPolicy`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "autoscaling:DescribeAutoScalingGroups",
        "backup:DescribeBackupVault",
        "backup:GetBackupPlan",
        "backup:GetBackupSelection",
        "backup:ListBackupPlans",
        "backup:ListBackupSelections",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "cloudformation:ValidateTemplate",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "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/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSResourceAccessManagerFullAccess

Deskripsi: Menyediakan akses penuh ke AWS Resource Access Manager

`AWSResourceAccessManagerFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSResourceAccessManagerFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 04 Juni 2019, 17:28 UTC
- Waktu yang telah diedit: 04 Juni 2019, 17:28 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceAccessManagerFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSResourceAccessManagerReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke AWS Resource Access Manager.

`AWSResourceAccessManagerReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSResourceAccessManagerReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 09 Desember 2019, 20:58 UTC
- Waktu yang telah diedit: 09 Desember 2019, 20:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceAccessManagerReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSResourceAccessManagerResourceShareParticipantAccess

Deskripsi: Menyediakan akses ke AWS Resource Access Manager yang APIs dibutuhkan oleh peserta berbagi sumber daya.

`AWSResourceAccessManagerResourceShareParticipantAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSResourceAccessManagerResourceShareParticipantAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 09 Desember 2019, 20:41 UTC
- Waktu yang telah diedit: 09 Desember 2019, 20:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceAccessManagerResourceShareParticipantAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ram:AcceptResourceShareInvitation",
        "ram:GetResourcePolicies",
        "ram:GetResourceShareInvitations",
        "ram:GetResourceShares",
        "ram:ListPendingInvitationResources",
        "ram:ListPrincipals",
        "ram:ListResources",
        "ram:RejectResourceShareInvitation"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSResourceAccessManagerServiceRolePolicy

Deskripsi: Kebijakan yang berisi akses Read-only AWS Resource Access Manager ke struktur Organizations pelanggan. Hal ini juga berisi izin IAM untuk menghapus peran.

`AWSResourceAccessManagerServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 14 November 2018, 19:28 UTC
- Waktu telah diedit: 14 November 2018, 19:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSResourceAccessManagerServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListChildren",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListRoots"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowDeletionOfServiceLinkedRoleForResourceAccessManager",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ram.amazonaws.com/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSResourceExplorerFullAccess

Deskripsi: Kebijakan ini memberikan izin administratif untuk mengakses sumber daya Resource Explorer dan memberikan izin hanya-baca ke layanan lain AWS untuk mendukung akses ini.

`AWSResourceExplorerFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSResourceExplorerFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 07 November 2022, 20:01 UTC
- Waktu telah diedit: 14 November 2023, 16:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceExplorerFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ResourceExplorerConsoleFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:*",
        "ec2:DescribeRegions",
        "ram:ListResources",
        "ram:GetResourceShares",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ResourceExplorerSLRAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "resource-explorer-2.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSResourceExplorerOrganizationsAccess

Deskripsi: Kebijakan ini memberikan izin administratif ke Resource Explorer dan memberikan izin hanya-baca ke layanan lain AWS untuk mendukung akses ini. Administrator AWS Organizations memerlukan izin ini untuk mengatur dan mengelola pencarian multi-akun di konsol.

`AWSResourceExplorerOrganizationsAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSResourceExplorerOrganizationsAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 14 November 2023, 17:01 UTC
- Waktu telah diedit: 14 November 2023, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceExplorerOrganizationsAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:*",
        "ec2:DescribeRegions",
        "ram:ListResources",
        "ram:GetResourceShares",
        "organizations:ListAccounts",
        "organizations:ListRoots",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAccountsForParent",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ResourceExplorerGetSLRAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/resource-
explorer-2.amazonaws.com/AWSServiceRoleForResourceExplorer"
    },
    {
      "Sid" : "ResourceExplorerCreateSLRAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "resource-explorer-2.amazonaws.com"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "OrganizationsAdministratorAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:DisableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "resource-explorer-2.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSResourceExplorerReadOnlyAccess

Deskripsi: Kebijakan ini memberikan izin hanya-baca untuk mencari dan melihat sumber daya Resource Explorer dan memberikan izin hanya-baca ke layanan lain untuk mendukung akses ini. AWS

`AWSResourceExplorerReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSResourceExplorerReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 07 November 2022, 19:56 UTC
- Waktu telah diedit: 14 November 2023, 16:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceExplorerReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ResourceExplorerReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:Get*",
        "resource-explorer-2:List*",
        "resource-explorer-2:Search",
        "resource-explorer-2:BatchGetView",
        "ec2:DescribeRegions",
        "ram:ListResources",
        "ram:GetResourceShares",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSResourceExplorerServiceRolePolicy

Deskripsi: Memungkinkan Resource Explorer untuk melihat sumber daya dan CloudTrail acara atas nama Anda untuk mengindeks sumber daya Anda untuk pencarian.

`AWSResourceExplorerServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 25 Oktober 2022, 20:35 UTC
- Waktu yang telah diedit: 23 Juni 2025, 10:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSResourceExplorerServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v14 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "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/*/deployments",
        "arn:aws:apigateway:*::/restapis/*/resources",
        "arn:aws:apigateway:*::/restapis/*/resources/*",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/vpclinks",
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*/routes",
        "arn:aws:apigateway:*::/apis/*/stages"
      ]
    },
    {
      "Sid" : "ResourceInventoryAccess",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:ListAnalyzers",
        "acm-pca:ListCertificateAuthorities",
        "acm:ListCertificates",
        "airflow:ListEnvironments",
```

```
        "amplify:ListApps",
        "amplify:ListBackendEnvironments",
        "amplify:ListBranches",
        "amplify:ListDomainAssociations",
        "amplifyuibuilder:ListComponents",
        "amplifyuibuilder:ListThemes",
        "app-integrations:ListEventIntegrations",
        "appconfig:ListApplications",
        "appconfig:ListDeploymentStrategies",
        "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:ListFrameworks",
        "backup:ListReportPlans",
        "batch:DescribeComputeEnvironments",
        "batch:DescribeJobDefinitions",
        "batch:DescribeJobQueues",
        "batch:ListSchedulingPolicies",
        "bedrock:ListAgents",
```

```
        "bedrock:ListBlueprints",
        "bedrock:ListCustomModels",
        "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: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",
        "config:DescribeConfigRules",
        "connect:ListHoursOfOperations",
        "connect:ListInstances",
        "connect:ListPhoneNumbersV2",
        "connect:ListQuickConnects",
        "connect:ListRules",
        "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:ListProjects",
        "devicefarm:ListTestGridProjects",
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeLags",
        "directconnect:DescribeVirtualInterfaces",
        "dms:DescribeCertificates",
        "dms:DescribeEndpoints",
        "dms:DescribeEventSubscriptions",
        "dms:DescribeReplicationInstances",
        "dms:DescribeReplicationSubnetGroups",
```

```
        "dms:DescribeReplicationTasks",
        "ds:DescribeDirectories",
        "dynamodb:ListStreams",
        "dynamodb:ListTables",
        "ec2:DescribeAddresses",
        "ec2:DescribeCapacityReservationFleets",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeCarrierGateways",
        "ec2:DescribeClientVpnEndpoints",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeElasticGpus",
        "ec2:DescribeExportImageTasks",
        "ec2:DescribeExportTasks",
        "ec2:DescribeFleets",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeFpgaImages",
        "ec2:DescribeHostReservations",
        "ec2:DescribeHosts",
        "ec2:DescribeImages",
        "ec2:DescribeImportImageTasks",
        "ec2:DescribeImportSnapshotTasks",
        "ec2:DescribeInstanceEventWindows",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeIpamPools",
        "ec2: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:DescribeVpcEndpointServices",
        "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",
        "ecs:ListTasks",
        "eks:ListAccessEntries",
        "eks:ListAddons",
        "eks:ListClusters",
        "eks:ListEksAnywhereSubscriptions",
        "eks:ListFargateProfiles",
        "eks:ListIdentityProviderConfigs",
```

```
        "eks:ListNodegroups",
        "eks:ListPodIdentityAssociations",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeCacheParameterGroups",
        "elasticache:DescribeCacheSecurityGroups",
        "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:DescribeFileSystems",
        "fsx:DescribeStorageVirtualMachines",
        "fsx:DescribeVolumes",
        "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:ListMLTransforms",
        "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:ListScenes",
        "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:ListPlaybackKeyPairs",
        "ivs:ListRecordingConfigurations",
```

```
        "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:ListStreamConsumers",
        "kinesis:ListStreams",
        "kinesisanalytics:ListApplications",
        "kinesisvideo:ListSignalingChannels",
        "kinesisvideo:ListStreams",
        "kms:ListAliases",
        "kms:ListKeys",
        "lambda:ListAliases",
        "lambda:ListCodeSigningConfigs",
        "lambda:ListEventSourceMappings",
        "lambda:ListFunctions",
        "lambda:ListLayerVersions",
        "lambda:ListLayers",
        "lex:ListBotAliases",
        "lex:ListBots",
        "license-manager:ListDistributedGrants",
        "lightsail:GetBuckets",
        "lightsail:GetCertificates",
        "lightsail:GetContainerServices",
        "lightsail:GetDisks",
        "logs:DescribeDestinations",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "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",
        "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",
        "networkmanager:DescribeGlobalNetworks",
        "networkmanager:GetDevices",
        "networkmanager:GetLinks",
        "networkmanager:ListAttachments",
        "networkmanager:ListCoreNetworks",
        "oam:ListSinks",
        "omics:ListReferenceStores",
        "omics:ListRunGroups",
        "omics:ListWorkflows",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListAccounts",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListRoots",
        "outposts:ListSites",
        "panorama:ListPackages",
        "personalize:ListDatasetGroups",
        "personalize:ListDatasets",
```

```
        "personalize:ListSchemas",
        "personalize:ListSolutions",
        "pipes:ListPipes",
        "profile:ListDomains",
        "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:DescribeScheduledActions",
        "redshift:DescribeSnapshotCopyGrants",
        "redshift:DescribeSnapshotSchedules",
        "redshift:DescribeUsageLimits",
        "refactor-spaces:ListApplications",
```

```
        "refactor-spaces:ListEnvironments",
        "refactor-spaces:ListRoutes",
        "refactor-spaces:ListServices",
        "rekognition:DescribeProjects",
        "resiliencehub:ListApps",
        "resiliencehub:ListResiliencyPolicies",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListViews",
        "resource-groups:ListGroups",
        "robomaker:ListRobotApplications",
        "robomaker:ListSimulationApplications",
        "route53-recovery-control-config:ListClusters",
        "route53-recovery-control-config:ListControlPanels",
        "route53-recovery-control-config:ListSafetyRules",
        "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",
        "sagemaker:ListActions",
        "sagemaker:ListAlgorithms",
        "sagemaker:ListAppImageConfigs",
        "sagemaker:ListApps",
        "sagemaker:ListArtifacts",
        "sagemaker:ListClusters",
        "sagemaker:ListCodeRepositories",
        "sagemaker:ListContexts",
        "sagemaker:ListDataQualityJobDefinitions",
        "sagemaker:ListDomains",
```

```
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListEndpoints",
        "sagemaker:ListExperiments",
        "sagemaker:ListFeatureGroups",
        "sagemaker:ListFlowDefinitions",
        "sagemaker:ListHubs",
        "sagemaker:ListHumanTaskUis",
        "sagemaker:ListImageVersions",
        "sagemaker:ListImages",
        "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:ListProjects",
        "sagemaker:ListSpaces",
        "sagemaker:ListStudioLifecycleConfigs",
        "sagemaker:ListTrialComponents",
        "sagemaker:ListTrials",
        "sagemaker:ListUserProfiles",
        "sagemaker:ListWorkforces",
        "sagemaker:ListWorkteams",
        "scheduler:ListScheduleGroups",
        "scheduler:ListSchedules",
        "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:DescribeAutomationExecutions",
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeMaintenanceWindowTargets",
        "ssm:DescribeMaintenanceWindowTasks",
        "ssm:DescribeMaintenanceWindows",
        "ssm:DescribeParameters",
        "ssm:DescribePatchBaselines",
        "ssm:DescribeSessions",
        "ssm:ListAssociations",
        "ssm:ListDocuments",
        "ssm:ListInventoryEntries",
        "ssm:ListResourceDataSync",
        "states:ListActivities",
        "states:ListStateMachines",
        "storagegateway:ListGateways",
        "synthetics:DescribeCanaries",
        "synthetics:ListGroups",
        "timestream:ListDatabases",
        "timestream:ListScheduledQueries",
        "transfer:ListAgreements",
        "transfer:ListCertificates",
        "transfer:ListConnectors",
        "transfer:ListProfiles",
        "transfer:ListServers",
        "transfer:ListUsers",
        "transfer:ListWorkflows",
        "wafv2:ListWebACLs",
        "wisdom:ListAssistants",
        "wisdom:listAssistantAssociations",
        "wisdom:listKnowledgeBases",
        "workspaces:DescribeConnectionAliases",
        "workspaces:DescribeWorkspaces",
        "xray:GetGroups"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSResourceGroupsReadOnlyAccess

Deskripsi: Ini adalah kebijakan baca saja untuk AWS Resource Groups

`AWSResourceGroupsReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSResourceGroupsReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 07 Maret 2018, 10:27 UTC
- Waktu yang telah diedit: 05 Februari 2019, 17:56 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceGroupsReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
        "resource-groups:Get*",
        "resource-groups:List*",
        "resource-groups:Search*",
        "tag:Get*",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcs",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeSnapshots",
        "elasticache:ListTagsForResource",
        "elasticbeanstalk:DescribeEnvironments",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:ListClusters",
        "glacier:ListVaults",
        "glacier:DescribeVault",
        "glacier:ListTagsForVault",
        "kinesis:ListStreams",
        "kinesis:DescribeStream",
        "kinesis:ListTagsForStream",
        "opsworks:DescribeStacks",
        "opsworks:ListTags",
        "rds:DescribeDBInstances",
        "rds:DescribeDBSnapshots",
        "rds:ListTagsForResource",
        "redshift:DescribeClusters",
        "redshift:DescribeTags",
        "route53domains:ListDomains",
        "route53:ListHealthChecks",
        "route53:GetHealthCheck",
        "route53:ListHostedZones",
        "route53:GetHostedZone",
        "route53:ListTagsForResource",
        "storagegateway:ListGateways",
        "storagegateway:DescribeGatewayInformation",
        "storagegateway:ListTagsForResource",
        "s3:ListAllMyBuckets",
        "s3:GetBucketTagging",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTags",
        "ssm:ListDocuments"
```

```
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSRoboMaker_FullAccess

Deskripsi: Menyediakan akses penuh ke AWS RoboMaker melalui AWS Management Console dan SDK. Juga menyediakan akses pilih ke layanan terkait (misalnya, S3, IAM).

`AWSRoboMaker_FullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSRoboMaker_FullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 10 September 2020, 18:34 UTC
- Waktu yang telah diedit: September 16, 2021, 21:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRoboMaker_FullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "robomaker:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "robomaker.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ecr:BatchGetImage",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "robomaker.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ecr-public:DescribeImages",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "robomaker.amazonaws.com"
        }
      }
```

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSRoboMakerReadOnlyAccess

Deskripsi: Menyediakan akses hanya baca AWS RoboMaker melalui AWS Management Console dan SDK

`AWSRoboMakerReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSRoboMakerReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 26 November 2018, 05:30 UTC
- Waktu yang telah diedit: 28 Agustus 2020, 23:10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRoboMakerReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : [
        "robomaker:List*",
        "robomaker:BatchDescribe*",
        "robomaker:Describe*",
        "robomaker:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSRoboMakerServicePolicy

Deskripsi: kebijakan RoboMaker layanan

`AWSRoboMakerServicePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 26 November 2018, 06:30 UTC
- Waktu yang telah diedit: 11 November 2021, 22:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSRoboMakerServicePolicy`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "greengrass:CreateDeployment",
        "greengrass:CreateGroupVersion",
        "greengrass:CreateFunctionDefinition",
        "greengrass:CreateFunctionDefinitionVersion",
        "greengrass:GetDeploymentStatus",
        "greengrass:GetGroup",
```

```
        "greengrass:GetGroupVersion",
        "greengrass:GetCoreDefinitionVersion",
        "greengrass:GetFunctionDefinitionVersion",
        "greengrass:GetAssociatedRole",
        "lambda:CreateFunction",
        "robomaker:CreateSimulationJob",
        "robomaker:CancelSimulationJob"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "robomaker:TagResource"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:robomaker:*:*:simulation-job/*"
    },
    {
      "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"
          ]
        }
```

```
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSRoboMakerServiceRolePolicy

Deskripsi: kebijakan RoboMaker layanan

`AWSRoboMakerServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSRoboMakerServiceRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 26 November 2018, 05:33 UTC
- Waktu telah diedit: 26 November 2018, 05:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRoboMakerServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "greengrass:CreateDeployment",
        "greengrass:CreateGroupVersion",
        "greengrass:CreateFunctionDefinition",
        "greengrass:CreateFunctionDefinitionVersion",
        "greengrass:GetDeploymentStatus",
        "greengrass:GetGroup",
        "greengrass:GetGroupVersion",
        "greengrass:GetCoreDefinitionVersion",
        "greengrass:GetFunctionDefinitionVersion",
        "greengrass:GetAssociatedRole",
        "lambda:CreateFunction"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "lambda:UpdateFunctionCode",
        "lambda:GetFunction",
        "lambda:UpdateFunctionConfiguration"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:lambda:*:*:function:aws-robomaker-*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
```

```
          "iam:PassedToService" : "lambda.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSRolesAnywhereServicePolicy

Deskripsi: Memungkinkan IAM Roles Anywhere untuk mempublikasikan metrik layanan/penggunaan ke CloudWatch dan memeriksa status Otoritas Sertifikat Pribadi atas nama Anda.

`AWSRolesAnywhereServicePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 05 Juli 2022, 15:26 UTC
- Waktu yang telah diedit: 05 Juli 2022, 15.26 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSRolesAnywhereServicePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/RolesAnywhere",
            "AWS/Usage"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:DescribeCertificateAuthority"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM

- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSS3OnOutpostsServiceRolePolicy

Deskripsi: Izinkan Amazon S3 pada layanan Outposts untuk mengelola sumber daya EC2 jaringan atas nama Anda.

`AWSS3OnOutpostsServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 03 Oktober 2023, 20:32 UTC
- Waktu telah diedit: 03 Oktober 2023, 20:32 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSS3OnOutpostsServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "ec2:DescribeCoipPools",
        "ec2:GetCoipPoolUsage",
        "ec2:DescribeAddresses",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations"
      ],
      "Resource" : "*",
      "Sid" : "DescribeVpcResources"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Sid" : "CreateNetworkInterface"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "S3 On Outposts"
        }
      },
      "Sid" : "CreateTagsForCreateNetworkInterface"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:ipv4pool-ec2/*"
      ],
      "Sid" : "AllocateIpAddress"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:elastic-ip/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "S3 On Outposts"
        }
      },
      "Sid" : "CreateTagsForAllocateIpAddress"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DisassociateAddress",
        "ec2:ReleaseAddress",
        "ec2:AssociateAddress"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "S3 On Outposts"
        }
      },
      "Sid" : "ReleaseVpcResources"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateNetworkInterface",
            "AllocateAddress"
          ],
          "aws:RequestTag/CreatedBy" : [
            "S3 On Outposts"
          ]
        }
      },
      "Sid" : "CreateTags"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSSavingsPlansFullAccess

Deskripsi: Menyediakan akses penuh ke layanan Savings Plans

`AWSSavingsPlansFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSSavingsPlansFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 November 2019, 22:45 UTC
- Waktu yang telah diedit: 06 November 2019, 22:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSavingsPlansFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSSavingsPlansReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke layanan Savings Plans

`AWSSavingsPlansReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSSavingsPlansReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 November 2019, 22:45 UTC
- Waktu yang telah diedit: 06 November 2019, 22:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSavingsPlansReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSSecurityHubFullAccess

Deskripsi: Menyediakan akses penuh untuk menggunakan AWS Security Hub.

`AWSSecurityHubFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSSecurityHubFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 November 2018, 23:54 UTC
- Waktu yang telah diedit: 17 Juni 2025, 13:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityHubFullAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "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",
        "inspector2:BatchGetAccountStatus",
        "pricing:GetProducts"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSSecurityHubOrganizationsAccess

Deskripsi: Memberikan izin untuk mengaktifkan dan mengelola AWS Security Hub dalam suatu organisasi. Termasuk mengaktifkan layanan di seluruh organisasi, dan menentukan akun administrator yang didelegasikan untuk layanan.

`AWSSecurityHubOrganizationsAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSSecurityHubOrganizationsAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 15 Maret 2021, 20:53 UTC
- Waktu yang telah diedit: 24 Juni 2025, 22:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityHubOrganizationsAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "OrganizationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:ListRoots",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAccountsForParent",
        "organizations:ListParents",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListPolicies",
```

```
        "organizations:ListPoliciesForTarget",
        "organizations:ListTargetsForPolicy"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationPermissionsEnable",
      "Effect" : "Allow",
      "Action" : "organizations:EnableAWSServiceAccess",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "securityhub.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "OrganizationPermissionsDelegatedAdmin",
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource" : "arn:aws:organizations::*:account/o-*/*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "securityhub.amazonaws.com"
        }
      }
    },
    {
      "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/*"
      ],
      "Condition" : {
        "StringLikeIfExists" : {
          "organizations:PolicyType" : "SECURITYHUB_POLICY"
        }
      }
    },
    {
      "Sid" : "OrganizationPolicyTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:TagResource",
        "organizations:UntagResource",
        "organizations:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:organizations::*:policy/o-*/securityhub_policy/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSSecurityHubReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke sumber daya AWS Security Hub

`AWSSecurityHubReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSSecurityHubReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 November 2018, 01:34 UTC
- Waktu telah diedit: 22 Februari 2024, 23:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityHubReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSSecurityHubServiceRolePolicy

Deskripsi: Peran terkait layanan yang diperlukan untuk AWS Security Hub untuk mengakses sumber daya Anda.

`AWSSecurityHubServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 27 November 2018, 23:47 UTC
- Waktu telah diedit: 27 November 2023, 03:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSecurityHubServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v14 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecurityHubServiceRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:GetEventSelectors",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "logs:DescribeMetricFilters",
        "sns:ListSubscriptionsByTopic",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:DescribeConfigRules",
        "config:DescribeConfigRuleEvaluationStatus",
        "config:BatchGetResourceConfig",
        "config:SelectResourceConfig",
        "iam:GenerateCredentialReport",
        "organizations:ListAccounts",
        "config:PutEvaluations",
        "tag:GetResources",
        "iam:GetCredentialReport",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListChildren",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "securityhub:BatchDisableStandards",
        "securityhub:BatchEnableStandards",
        "securityhub:BatchUpdateStandardsControlAssociations",
        "securityhub:BatchGetSecurityControls",
        "securityhub:BatchGetStandardsControlAssociations",
        "securityhub:CreateMembers",
        "securityhub:DeleteMembers",
        "securityhub:DescribeHub",
        "securityhub:DescribeOrganizationConfiguration",
        "securityhub:DescribeStandards",
        "securityhub:DescribeStandardsControls",
```

```
        "securityhub:DisassociateFromAdministratorAccount",
        "securityhub:DisassociateMembers",
        "securityhub:DisableSecurityHub",
        "securityhub:EnableSecurityHub",
        "securityhub:GetEnabledStandards",
        "securityhub:ListStandardsControlAssociations",
        "securityhub:ListSecurityControlDefinitions",
        "securityhub:UpdateOrganizationConfiguration",
        "securityhub:UpdateSecurityControl",
        "securityhub:UpdateSecurityHubConfiguration",
        "securityhub:UpdateStandardsControl"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityHubServiceRoleConfigPermissions",
      "Effect" : "Allow",
      "Action" : [
        "config:PutConfigRule",
        "config:DeleteConfigRule",
        "config:GetComplianceDetailsByConfigRule"
      ],
      "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/*securityhub*"
    },
    {
      "Sid" : "SecurityHubServiceRoleOrganizationsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "securityhub.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSSecurityHubV2ServiceRolePolicy

Deskripsi: Kebijakan ini memungkinkan Security Hub mengelola aturan AWS Config dan sumber daya Security Hub di organisasi dan atas nama Anda.

`AWSSecurityHubV2ServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 10 Juni 2025, 17:37 UTC
- Waktu yang telah diedit: 10 Juni 2025, 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSecurityHubV2ServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSSecurityIncidentResponseCaseFullAccess

Deskripsi: Kebijakan memberi pelanggan izin Baca dan Tulis untuk sumber daya kasus yang dibuat melalui layanan Respons Insiden Keamanan.

`AWSSecurityIncidentResponseCaseFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSSecurityIncidentResponseCaseFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Desember 2024, 23:21 UTC
- Waktu telah diedit: 01 Desember 2024, 23:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityIncidentResponseCaseFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSSecurityIncidentResponseFullAccess

Deskripsi: Kebijakan memberi pelanggan izin Baca dan Tulis ke semua sumber daya yang terkait dengan layanan Respons Insiden Keamanan.

`AWSSecurityIncidentResponseFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSSecurityIncidentResponseFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Desember 2024, 23:21 UTC
- Waktu telah diedit: 01 Desember 2024, 23:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityIncidentResponseFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSSecurityIncidentResponseReadOnlyAccess

Deskripsi: Kebijakan memberi pelanggan izin hanya-baca untuk semua sumber daya yang terkait dengan layanan Respons Insiden Keamanan. Izin termasuk akses GetCaseAttachmentDownloadUrl juga untuk kemampuan untuk mendapatkan unduhan lampiran kasus URLs.

`AWSSecurityIncidentResponseReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSSecurityIncidentResponseReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Desember 2024, 23:06 UTC
- Waktu yang telah diedit: 01 Desember 2024, 23:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityIncidentResponseReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSSecurityIncidentResponseServiceRolePolicy

Deskripsi: Menyediakan akses ke AWS Sumber Daya yang dikelola atau digunakan oleh Security Incident Response

`AWSSecurityIncidentResponseServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 01 Desember 2024, 16:36 UTC
- Waktu telah diedit: 01 Desember 2024, 16:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSecurityIncidentResponseServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
        "organizations:ListAccounts",
        "organizations:ListChildren"
      ],
      "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/*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSSecurityIncidentResponseTriageServiceRolePolicy

Deskripsi: Menyediakan akses ke Respons Insiden AWS Keamanan untuk terus memantau lingkungan Anda untuk ancaman keamanan, menyesuaikan layanan keamanan untuk mengurangi kebisingan peringatan, dan mengumpulkan informasi untuk menyelidiki potensi insiden.

`AWSSecurityIncidentResponseTriageServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 01 Desember 2024, 16:36 UTC
- Waktu yang telah diedit: 02 Juni 2025, 18:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSecurityIncidentResponseTriageServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSServiceCatalogAdminFullAccess

Deskripsi: Menyediakan akses penuh ke kemampuan admin katalog layanan

`AWSServiceCatalogAdminFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSServiceCatalogAdminFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 15 Februari 2018, 17:19 UTC
- Waktu yang telah diedit: 13 April 2023, 18:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogAdminFullAccess`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks",
        "cloudformation:SetStackPolicy",
        "cloudformation:UpdateStack",
```

```
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:ListChangeSets",
        "cloudformation:DeleteChangeSet",
        "cloudformation:ListStackResources",
        "cloudformation:TagResource",
        "cloudformation:CreateStackSet",
        "cloudformation:CreateStackInstances",
        "cloudformation:UpdateStackSet",
        "cloudformation:UpdateStackInstances",
        "cloudformation:DeleteStackSet",
        "cloudformation:DeleteStackInstances",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:ListStackInstances",
        "cloudformation:ListStackSetOperations",
        "cloudformation:ListStackSetOperationResults"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/SC-*",
        "arn:aws:cloudformation:*:*:stack/StackSet-SC-*",
        "arn:aws:cloudformation:*:*:changeSet/SC-*",
        "arn:aws:cloudformation:*:*:stackset/SC-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateUploadBucket",
        "cloudformation:GetTemplateSummary",
        "cloudformation:ValidateTemplate",
        "iam:GetGroup",
        "iam:GetRole",
        "iam:GetUser",
        "iam:ListGroups",
        "iam:ListRoles",
        "iam:ListUsers",
        "servicecatalog:Get*",
        "servicecatalog:Scan*",
        "servicecatalog:Search*",
        "servicecatalog:List*",
        "servicecatalog:TagResource",
```

```
        "servicecatalog:UntagResource",
        "servicecatalog:SyncResource",
        "ssm:DescribeDocument",
        "ssm:GetAutomationExecution",
        "ssm:ListDocuments",
        "ssm:ListDocumentVersions",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:Accept*",
        "servicecatalog:Associate*",
        "servicecatalog:Batch*",
        "servicecatalog:Copy*",
        "servicecatalog:Create*",
        "servicecatalog:Delete*",
        "servicecatalog:Describe*",
        "servicecatalog:Disable*",
        "servicecatalog:Disassociate*",
        "servicecatalog:Enable*",
        "servicecatalog:Execute*",
        "servicecatalog:Import*",
        "servicecatalog:Provision*",
        "servicecatalog:Put*",
        "servicecatalog:Reject*",
        "servicecatalog:Terminate*",
        "servicecatalog:Update*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "servicecatalog.amazonaws.com"
        }
      }
    },
```

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSServiceCatalogAdminReadOnlyAccess

Deskripsi: Menyediakan akses read-only ke kemampuan admin Service Catalog

`AWSServiceCatalogAdminReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSServiceCatalogAdminReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 25 Oktober 2019, 18:53 UTC
- Waktu yang telah diedit: 25 Oktober 2019, 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogAdminReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ListChangeSets",
        "cloudformation:ListStackResources",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:ListStackInstances",
        "cloudformation:ListStackSetOperations",
        "cloudformation:ListStackSetOperationResults"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/SC-*",
        "arn:aws:cloudformation:*:*:stack/StackSet-SC-*",
        "arn:aws:cloudformation:*:*:changeSet/SC-*",
        "arn:aws:cloudformation:*:*:stackset/SC-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:GetTemplateSummary",
        "iam:GetGroup",
        "iam:GetRole",
        "iam:GetUser",
        "iam:ListGroups",
```

```
        "iam:ListRoles",
        "iam:ListUsers",
        "servicecatalog:Get*",
        "servicecatalog:List*",
        "servicecatalog:Describe*",
        "servicecatalog:ScanProvisionedProducts",
        "servicecatalog:Search*",
        "ssm:DescribeDocument",
        "ssm:GetAutomationExecution",
        "ssm:ListDocuments",
        "ssm:ListDocumentVersions",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSServiceCatalogAppRegistryFullAccess

Deskripsi: Menyediakan akses penuh ke kemampuan Service Catalog App Registry

`AWSServiceCatalogAppRegistryFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSServiceCatalogAppRegistryFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 12 November 2020, 22:25 UTC
- Waktu telah diedit: 07 Desember 2023, 21:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogAppRegistryFullAccess`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AppRegistryUpdateStackAndResourceGroupTagging",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:UpdateStack",
        "tag:GetResources"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "servicecatalog-appregistry.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AppRegistryResourceGroupsIntegration",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:DeleteGroup",
        "resource-groups:GetGroup",
        "resource-groups:GetTags",
        "resource-groups:Tag",
        "resource-groups:Untag",
```

```
        "resource-groups:GetGroupConfiguration",
        "resource-groups:AssociateResource",
        "resource-groups:DisassociateResource"
      ],
      "Resource" : "arn:aws:resource-groups:*:*:group/AWS_*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "servicecatalog-appregistry.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AppRegistryServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/servicecatalog-
appregistry.amazonaws.com/AWSServiceRoleForAWSServiceCatalogAppRegistry*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "servicecatalog-appregistry.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AppRegistryOperations",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "servicecatalog:CreateApplication",
        "servicecatalog:GetApplication",
        "servicecatalog:UpdateApplication",
        "servicecatalog:DeleteApplication",
        "servicecatalog:ListApplications",
        "servicecatalog:AssociateResource",
        "servicecatalog:DisassociateResource",
        "servicecatalog:GetAssociatedResource",
        "servicecatalog:ListAssociatedResources",
        "servicecatalog:AssociateAttributeGroup",
        "servicecatalog:DisassociateAttributeGroup",
        "servicecatalog:ListAssociatedAttributeGroups",
        "servicecatalog:CreateAttributeGroup",
        "servicecatalog:UpdateAttributeGroup",
        "servicecatalog:DeleteAttributeGroup",
        "servicecatalog:GetAttributeGroup",
```

```
        "servicecatalog:ListAttributeGroups",
        "servicecatalog:SyncResource",
        "servicecatalog:ListAttributeGroupsForApplication",
        "servicecatalog:GetConfiguration",
        "servicecatalog:PutConfiguration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AppRegistryResourceTagging",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:ListTagsForResource",
        "servicecatalog:UntagResource",
        "servicecatalog:TagResource"
      ],
      "Resource" : "arn:aws:servicecatalog:*:*:*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSServiceCatalogAppRegistryReadOnlyAccess

Deskripsi: Menyediakan akses hanya-baca ke kemampuan Registri Aplikasi Service Catalog

`AWSServiceCatalogAppRegistryReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSServiceCatalogAppRegistryReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 12 November 2020, 22:34 UTC
- Waktu yang telah diedit: 17 November 2022, 18.16 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogAppRegistryReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:GetApplication",
        "servicecatalog:ListApplications",
        "servicecatalog:GetAssociatedResource",
        "servicecatalog:ListAssociatedResources",
        "servicecatalog:ListAssociatedAttributeGroups",
        "servicecatalog:GetAttributeGroup",
        "servicecatalog:ListAttributeGroups",
        "servicecatalog:ListTagsForResource",
        "servicecatalog:ListAttributeGroupsForApplication",
        "servicecatalog:GetConfiguration"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSServiceCatalogAppRegistryServiceRolePolicy

Deskripsi: Memungkinkan Service Catalog AppRegistry mengelola Resource Groups atas nama Anda

`AWSServiceCatalogAppRegistryServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 18 Mei 2021 22:18 UTC
- Waktu yang telah diedit: 26 Oktober 2022, 16.05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogAppRegistryServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "cloudformation:DescribeStacks",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:Tag"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/EnableAWSServiceCatalogAppRegistry" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:DeleteGroup",
        "resource-groups:UpdateGroup",
        "resource-groups:GetTags",
        "resource-groups:Tag",
        "resource-groups:Untag"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/EnableAWSServiceCatalogAppRegistry" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:GetGroup",
```

```
        "resource-groups:GetGroupConfiguration"
      ],
      "Resource" : [
        "arn:*:resource-groups:*:*:group/AWS_AppRegistry*",
        "arn:*:resource-groups:*:*:group/AWS_CloudFormation_Stack*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSServiceCatalogEndUserFullAccess

Deskripsi: Menyediakan akses penuh ke kemampuan enduser katalog layanan

`AWSServiceCatalogEndUserFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSServiceCatalogEndUserFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 15 Februari 2018, 17:22 UTC
- Waktu yang telah diedit: 10 Juli 2019, 20:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogEndUserFullAccess`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks",
        "cloudformation:SetStackPolicy",
        "cloudformation:ValidateTemplate",
        "cloudformation:UpdateStack",
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:ListChangeSets",
        "cloudformation:DeleteChangeSet",
        "cloudformation:TagResource",
        "cloudformation:CreateStackSet",
        "cloudformation:CreateStackInstances",
        "cloudformation:UpdateStackSet",
        "cloudformation:UpdateStackInstances",
        "cloudformation:DeleteStackSet",
        "cloudformation:DeleteStackInstances",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:ListStackInstances",
        "cloudformation:ListStackResources",
        "cloudformation:ListStackSetOperations",
        "cloudformation:ListStackSetOperationResults"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/SC-*",
        "arn:aws:cloudformation:*:*:stack/StackSet-SC-*",
        "arn:aws:cloudformation:*:*:changeSet/SC-*",
```

```
        "arn:aws:cloudformation:*:*:stackset/SC-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:GetTemplateSummary",
        "servicecatalog:DescribeProduct",
        "servicecatalog:DescribeProductView",
        "servicecatalog:DescribeProvisioningParameters",
        "servicecatalog:ListLaunchPaths",
        "servicecatalog:ProvisionProduct",
        "servicecatalog:SearchProducts",
        "ssm:DescribeDocument",
        "ssm:GetAutomationExecution",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:DescribeProvisionedProduct",
        "servicecatalog:DescribeRecord",
        "servicecatalog:ListRecordHistory",
        "servicecatalog:ListStackInstancesForProvisionedProduct",
        "servicecatalog:ScanProvisionedProducts",
        "servicecatalog:TerminateProvisionedProduct",
        "servicecatalog:UpdateProvisionedProduct",
        "servicecatalog:SearchProvisionedProducts",
        "servicecatalog:CreateProvisionedProductPlan",
        "servicecatalog:DescribeProvisionedProductPlan",
        "servicecatalog:ExecuteProvisionedProductPlan",
        "servicecatalog:DeleteProvisionedProductPlan",
        "servicecatalog:ListProvisionedProductPlans",
        "servicecatalog:ListServiceActionsForProvisioningArtifact",
        "servicecatalog:ExecuteProvisionedProductServiceAction",
        "servicecatalog:DescribeServiceActionExecutionParameters"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "servicecatalog:userLevel" : "self"
```

```
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSServiceCatalogEndUserReadOnlyAccess

Deskripsi: Menyediakan akses read-only ke kemampuan pengguna akhir Service Catalog

`AWSServiceCatalogEndUserReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSServiceCatalogEndUserReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 25 Oktober 2019, 18:49 UTC
- Waktu yang telah diedit: 25 Oktober 2019, 18:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogEndUserReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ListChangeSets",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:ListStackInstances",
        "cloudformation:ListStackResources",
        "cloudformation:ListStackSetOperations",
        "cloudformation:ListStackSetOperationResults"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/SC-*",
        "arn:aws:cloudformation:*:*:stack/StackSet-SC-*",
        "arn:aws:cloudformation:*:*:changeSet/SC-*",
        "arn:aws:cloudformation:*:*:stackset/SC-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:GetTemplateSummary",
        "servicecatalog:DescribeProduct",
        "servicecatalog:DescribeProductView",
        "servicecatalog:DescribeProvisioningParameters",
        "servicecatalog:ListLaunchPaths",
        "servicecatalog:SearchProducts",
        "ssm:DescribeDocument",
        "ssm:GetAutomationExecution",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:DescribeProvisionedProduct",
        "servicecatalog:DescribeRecord",
        "servicecatalog:ListRecordHistory",
        "servicecatalog:ListStackInstancesForProvisionedProduct",
        "servicecatalog:ScanProvisionedProducts",
        "servicecatalog:SearchProvisionedProducts",
        "servicecatalog:DescribeProvisionedProductPlan",
        "servicecatalog:ListProvisionedProductPlans",
        "servicecatalog:ListServiceActionsForProvisioningArtifact",
        "servicecatalog:DescribeServiceActionExecutionParameters"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "servicecatalog:userLevel" : "self"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSServiceCatalogOrgsDataSyncServiceRolePolicy

Deskripsi: Kebijakan Peran Tertaut Layanan AWS ServiceCatalog untuk disinkronkan dengan struktur AWS organisasi Organizations

`AWSServiceCatalogOrgsDataSyncServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 10 April 2023, 20:48 UTC
- Waktu telah diedit: 10 April 2023, 20:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogOrgsDataSyncServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "OrganizationsDataSyncToServiceCatalog",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSServiceCatalogSyncServiceRolePolicy

Deskripsi: Peran Tertaut Layanan AWS ServiceCatalog untuk menyinkronkan Artefak Penyediaan dari repositori sumber

`AWSServiceCatalogSyncServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 15 November 2022, 21:20 UTC
- Waktu yang telah diedit: 03 Mei 2024, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogSyncServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ArtifactSyncToServiceCatalog",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:ListProvisioningArtifacts",
        "servicecatalog:DescribeProductAsAdmin",
        "servicecatalog:DeleteProvisioningArtifact",
        "servicecatalog:ListServiceActionsForProvisioningArtifact",
        "servicecatalog:DescribeProvisioningArtifact",
        "servicecatalog:CreateProvisioningArtifact",
        "servicecatalog:UpdateProvisioningArtifact"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AccessArtifactRepositories",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection",
        "codeconnections:UseConnection"
      ],
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ]
    },
    {
      "Sid" : "ValidateTemplate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ValidateTemplate"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSServiceRoleForAmazonEKSNodegroup

Deskripsi: Izin diperlukan untuk mengelola nodegroup di akun pelanggan. Kebijakan ini terkait dengan pengelolaan sumber daya berikut: AutoscalingGroups, SecurityGroups, LaunchTemplates dan InstanceProfiles.

`AWSServiceRoleForAmazonEKSNodegroup`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 07 November 2019, 01:34 UTC
- Waktu yang telah diedit: 21 November 2024, 00:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForAmazonEKSNodegroup`

Versi kebijakan

Versi kebijakan: v10 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SharedSecurityGroupRelatedPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DescribeInstances",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/eks" : "*"
        }
      }
    },
    {
      "Sid" : "EKSCreatedSecurityGroupRelatedPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DescribeInstances",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/eks:nodegroup-name" : "*"
        }
      }
    },
    {
      "Sid" : "LaunchTemplateRelatedPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/eks:nodegroup-name" : "*"
        }
      }
    },
    {
      "Sid" : "AutoscalingRelatedPermissions",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:UpdateAutoScalingGroup",
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:TerminateInstanceInAutoScalingGroup",
        "autoscaling:CompleteLifecycleAction",
        "autoscaling:PutLifecycleHook",
        "autoscaling:PutNotificationConfiguration",
        "autoscaling:EnableMetricsCollection",
        "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/*"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSServiceRoleForAmazonQDeveloper

Deskripsi: Peran Tertaut Layanan ini memberikan kemampuan Pengembang Amazon Q untuk memberikan informasi penggunaan.

`AWSServiceRoleForAmazonQDeveloper`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan

- Waktu pembuatan: 25 April 2024, 07:40 UTC
- Waktu telah diedit: 25 April 2024, 07:40 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForAmazonQDeveloper`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "sid1",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/Q"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSServiceRoleForAWSTransform

Deskripsi: Peran Tertaut Layanan ini memberi AWS Transform kemampuan untuk memberikan informasi penggunaan.

`AWSServiceRoleForAWSTransform`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 15 Mei 2025, 13:37 UTC
- Waktu yang telah diedit: 15 Mei 2025, 13:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForAWSTransform`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/Transform"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy

Deskripsi: Menyediakan akses ke sumber daya Systems Manager yang digunakan oleh CloudWatch Alarm

`AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 01 Oktober 2020, 09:49 UTC
- Waktu telah diedit: 01 Oktober 2020, 09:49 UTC

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

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePoli

Deskripsi: Memungkinkan CloudWatch untuk mengakses metrik Performance Insights RDS atas nama Anda

`AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 07 September 2023, 09:32 UTC
- Waktu telah diedit: 07 September 2023, 09:32 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "pi:GetResourceMetrics"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSServiceRoleForCodeGuru-Profiler

Deskripsi: Peran terkait layanan yang diperlukan Amazon CodeGuru Profiler untuk mengirim pemberitahuan atas nama Anda.

`AWSServiceRoleForCodeGuru-Profiler`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 26 Juni 2020, 22:04 UTC
- Waktu yang telah diedit: 26 Juni 2020, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCodeGuru-Profiler`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSServiceRoleForCodeWhispererPolicy

Deskripsi: Peran ini memberikan izin CodeWhisperer untuk mengakses data di akun Anda untuk menghitung penagihan, menyediakan akses untuk membuat dan mengakses laporan keamanan di Amazon CodeGuru, dan memancarkan data ke akun Anda. CloudWatch

`AWSServiceRoleForCodeWhispererPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 24 Maret 2023, 19:39 UTC

- Waktu telah diedit: 29 Maret 2024, 22:13 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCodeWhispererPolicy`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "sid1",
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:ListMembersInGroup"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "sid2",
      "Effect" : "Allow",
      "Action" : [
        "sso:ListProfileAssociations",
        "sso:ListProfiles",
        "sso:ListDirectoryAssociations",
        "sso:DescribeRegisteredRegions",
        "sso:GetProfile",
        "sso:GetManagedApplicationInstance",
        "sso:ListApplicationAssignments",
        "sso:DescribeInstance",
        "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"
          ]
        }
      }
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSServiceRoleForEC2ScheduledInstances

Deskripsi: Memungkinkan Instans EC2 Terjadwal untuk meluncurkan dan mengelola instans spot.

`AWSServiceRoleForEC2ScheduledInstances`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 12 Oktober 2017, 18:31 UTC
- Waktu yang telah diedit: 12 Oktober 2017, 18:31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForEC2ScheduledInstances`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws:ec2sri:scheduledInstanceId"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:ec2sri:scheduledInstanceId" : "*"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy

Deskripsi: AWS GroundStation menggunakan peran terkait layanan ini untuk memanggil EC2 untuk menemukan alamat publik IPv4

`AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 13 Desember 2022, 23:52 UTC
- Waktu yang telah diedit: 13 Desember 2022, 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      "Action" : [
        "ec2:DescribeAddresses",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSServiceRoleForImageBuilder

Deskripsi: Memungkinkan EC2 ImageBuilder untuk memanggil AWS layanan atas nama Anda.

`AWSServiceRoleForImageBuilder`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 29 November 2019, 22:02 UTC
- Waktu yang telah diedit: 26 Desember 2024, 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForImageBuilder`

Versi kebijakan

Versi kebijakan: v20 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSServiceRoleForIoTSiteWise

Deskripsi: Memungkinkan AWS IoT SiteWise untuk menyediakan dan mengelola gateway serta data kueri. Kebijakan ini mencakup izin AWS Greengrass yang diperlukan untuk diterapkan ke grup, izin AWS Lambda untuk membuat dan memperbarui fungsi awalan layanan, dan izin IoT Analytics untuk kueri data dari datastores. AWS

`AWSServiceRoleForIoTSiteWise`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 14 November 2018, 19:19 UTC
- Waktu telah diedit: 13 November 2023, 18:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForIoTSiteWise`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSiteWiseReadGreenGrass",
      "Effect" : "Allow",
      "Action" : [
        "greengrass:GetAssociatedRole",
        "greengrass:GetCoreDefinition",
        "greengrass:GetCoreDefinitionVersion",
        "greengrass:GetGroup",
        "greengrass:GetGroupVersion"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSiteWiseAccessLogGroup",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/iotsitewise*"
    },
    {
      "Sid" : "AllowSiteWiseAccessLog",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/iotsitewise*:log-stream:*"
    },
    {
      "Sid" : "AllowSiteWiseAccessSiteWiseManagedWorkspaceInTwinMaker",
      "Effect" : "Allow",
```

```
      "Action" : [
        "iottwinmaker:GetWorkspace",
        "iottwinmaker:ExecuteQuery"
      ],
      "Resource" : "arn:aws:iottwinmaker:*:*:workspace/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "iottwinmaker:linkedServices" : [
            "IOTSITEWISE"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSServiceRoleForLogDeliveryPolicy

Deskripsi: Memungkinkan layanan Pengiriman Log untuk mengirimkan log dengan memanggil tujuan log atas nama Anda.

`AWSServiceRoleForLogDeliveryPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 04 Oktober 2019, 17:31 UTC
- Waktu telah diedit: 16 Januari 2025, 21:37 UTC

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

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LogDeliveryToFirehose",
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch",
        "firehose:ListTagsForDeliveryStream"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/LogDeliveryEnabled" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSServiceRoleForMonitronPolicy

Deskripsi: Memberikan izin Amazon Monitron untuk AWS mengelola sumber daya, AWS termasuk penetapan pengguna SSO atas nama Anda.

`AWSServiceRoleForMonitronPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 02 Desember 2020, 19:06 UTC
- Waktu yang telah diedit: 02 Oktober 2024, 10:06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForMonitronPolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSServiceRoleForNeptuneGraphPolicy

Deskripsi: Menyediakan akses Cloudwatch untuk mempublikasikan metrik operasional dan penggunaan serta log untuk Amazon Neptunus

`AWSServiceRoleForNeptuneGraphPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 29 November 2023, 14:03 UTC
- Waktu telah diedit: 29 November 2023, 14:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForNeptuneGraphPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GraphMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/Neptune",
            "AWS/Usage"
          ]
        }
      }
    },
    {
      "Sid" : "GraphLogGroup",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/neptune/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Sid" : "GraphLogEvents",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/neptune/*:log-stream:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSServiceRoleForPrivateMarketplaceAdminPolicy

Deskripsi: Memberikan izin untuk mendeskripsikan dan memperbarui sumber daya Private Marketplace dan mendeskripsikan AWS Organizations

`AWSServiceRoleForPrivateMarketplaceAdminPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 14 Februari 2024, 22:28 UTC
- Waktu telah diedit: 14 Februari 2024, 22:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForPrivateMarketplaceAdminPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PrivateMarketplaceCatalogDescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/Experience/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/Audience/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ProcurementPolicy/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/BrandingSettings/*"
      ]
    },
    {
      "Sid" : "PrivateMarketplaceCatalogDescribeChangeSetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeChangeSet"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "PrivateMarketplaceCatalogListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListEntities",
        "aws-marketplace:ListChangeSets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PrivateMarketplaceStartChangeSetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:StartChangeSet"
      ],
      "Condition" : {
        "StringEquals" : {
          "catalog:ChangeType" : [
            "AssociateAudience",
            "DisassociateAudience"
          ]
        }
      },
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/Experience/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ChangeSet/*"
      ]
    },
    {
      "Sid" : "PrivateMarketplaceOrganizationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListChildren"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSServiceRoleForProcurementInsightsPolicy

Deskripsi: Kebijakan Wawasan Pengadaan untuk mendapatkan detail Akun Organisasi

`AWSServiceRoleForProcurementInsightsPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 03 Oktober 2024, 14:26 UTC
- Waktu yang telah diedit: 03 Oktober 2024, 14:26 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForProcurementInsightsPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ProcurementInsightsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSServiceRoleForSMS

Deskripsi: Menyediakan akses ke AWS layanan dan sumber daya yang diperlukan untuk memigrasikan instans layanan ke AWS termasuk EC2, S3, dan Cloudformation.

`AWSServiceRoleForSMS`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 06 Agustus 2019, 18:39 UTC
- Waktu yang telah diedit: 15 Oktober 2020, 17:28 UTC

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

Versi kebijakan

Versi kebijakan: v10 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:CreateStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/sms-app-*/*",
      "Condition" : {
        "Null" : {
          "cloudformation:ResourceTypes" : "false"
        },
        "ForAllValues:StringEquals" : {
          "cloudformation:ResourceTypes" : [
            "AWS::EC2::Instance",
            "AWS::ApplicationInsights::Application",
            "AWS::ResourceGroups::Group"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DeleteStack",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:DescribeChangeSet",
```

```
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources",
        "cloudformation:GetTemplate"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/sms-app-*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ValidateTemplate",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteObject",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:PutLifecycleConfiguration"
      ],
      "Resource" : "arn:aws:s3:::sms-app-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sms:CreateReplicationJob",
        "sms:DeleteReplicationJob",
        "sms:GetReplicationJobs",
        "sms:GetReplicationRuns",
        "sms:GetServers",
        "sms:ImportServerCatalog",
        "sms:StartOnDemandReplicationRun",
        "sms:UpdateReplicationJob"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ssm:*::document/AWS-RunRemoteScript",
        "arn:aws:s3:::sms-app-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "ssm:resourceTag/UseForSMSApplicationValidation" : [
            "true"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CancelCommand",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CopySnapshot"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CopySnapshot",
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
```

```
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/SMSJobId" : [
            "sms-*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotAttribute",
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/SMSJobId" : [
            "sms-*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopyImage",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSnapshotAttribute",
        "ec2:DeregisterImage",
        "ec2:ImportImage",
        "ec2:DescribeImportImageTasks",
        "ec2:GetEbsEncryptionByDefault"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetInstanceProfile"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DisassociateIamInstanceProfile",
        "ec2:AssociateIamInstanceProfile",
        "ec2:ReplaceIamInstanceProfileAssociation"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/sms-app-*/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "iam:PassedToService" : "cloudformation.amazonaws.com"
        },
        "StringLike" : {
          "iam:AssociatedResourceArn" : "arn:aws:cloudformation:*:*:stack/sms-app-*/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyInstanceAttribute",
        "ec2:StopInstances",
        "ec2:StartInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/sms-app-*/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "applicationinsights:Describe*",
        "applicationinsights:List*",
        "cloudformation:ListStackResources"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "applicationinsights:CreateApplication",
        "applicationinsights:CreateComponent",
        "applicationinsights:UpdateApplication",
        "applicationinsights:DeleteApplication",
        "applicationinsights:UpdateComponentConfiguration",
```

```
        "applicationinsights:DeleteComponent"
      ],
      "Resource" : "arn:aws:applicationinsights:*:*:application/resource-group/sms-app-
*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:GetGroup",
        "resource-groups:UpdateGroup",
        "resource-groups:DeleteGroup"
      ],
      "Resource" : "arn:aws:resource-groups:*:*:group/sms-app-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/aws:cloudformation:stack-id" :
 "arn:aws:cloudformation:*:*:stack/sms-app-*/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/application-insights.amazonaws.com/
AWSServiceRoleForApplicationInsights"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "application-insights.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSServiceRoleForUserSubscriptions

Deskripsi: Menyediakan akses ke layanan Langganan Pengguna ke sumber daya Pusat Identitas Anda untuk memperbarui langganan Anda secara otomatis.

`AWSServiceRoleForUserSubscriptions`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 25 April 2024, 16:14 UTC
- Waktu telah diedit: 21 Februari 2025, 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForUserSubscriptions`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSServiceRolePolicyForBackupReports

Deskripsi: Menyediakan izin AWS Backup untuk membuat laporan kepatuhan atas nama Anda

`AWSServiceRolePolicyForBackupReports`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 19 Agustus 2021 21:16 UTC

- Waktu yang telah diedit: 10 Maret 2023, 00:51 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRolePolicyForBackupReports`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "backup:DescribeFramework",
        "backup:ListBackupJobs",
        "backup:ListRestoreJobs",
        "backup:ListCopyJobs"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:BatchGetResourceConfig",
        "config:SelectResourceConfig",
        "config:DescribeConfigurationAggregators",
        "config:SelectAggregateResourceConfig",
        "config:DescribeConfigRuleEvaluationStatus",
        "config:DescribeConfigRules",
        "s3:GetBucketLocation"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:GetComplianceDetailsByConfigRule",
        "config:PutConfigRule",
        "config:DeleteConfigRule"
      ],
      "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/
backup.amazonaws.com*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DeleteConfigurationAggregator",
        "config:PutConfigurationAggregator"
      ],
      "Resource" : "arn:aws:config:*:*:config-aggregator/aws-service-config-aggregator/
backup.amazonaws.com*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSServiceRolePolicyForBackupRestoreTesting

Deskripsi: Kebijakan ini berisi izin untuk pengujian pemulihan dan untuk membersihkan sumber daya yang dibuat selama pengujian.

`AWSServiceRolePolicyForBackupRestoreTesting`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 10 November 2023, 23:37 UTC
- Waktu telah diedit: 14 Februari 2024, 22:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRolePolicyForBackupRestoreTesting`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BackupActions",
      "Effect" : "Allow",
      "Action" : [
        "backup:DescribeRecoveryPoint",
        "backup:DescribeRestoreJob",
        "backup:DescribeProtectedResource",
        "backup:GetRecoveryPointRestoreMetadata",
        "backup:ListBackupVaults",
        "backup:ListProtectedResources",
        "backup:ListProtectedResourcesByBackupVault",
        "backup:ListRecoveryPointsByBackupVault",
        "backup:ListRecoveryPointsByResource",
        "backup:ListTags",
        "backup:StartRestoreJob"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "IamPassRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "backup.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshotTierStatus",
        "ec2:DescribeTags",
        "ec2:DescribeVolumes",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets",
        "fsx:DescribeFileSystems",
        "fsx:DescribeVolumes",
        "fsx:ListTagsForResource",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstanceAutomatedBackups",
        "rds:DescribeDBClusterAutomatedBackups",
        "rds:ListTagsForResource",
        "redshift:DescribeClusters"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DeleteActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume",
        "ec2:TerminateInstances",
        "elasticfilesystem:DeleteFilesystem",
        "elasticfilesystem:DeleteMountTarget",
        "rds:DeleteDBCluster",
        "rds:DeleteDBInstance",
        "fsx:DeleteFileSystem",
        "fsx:DeleteVolume"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/awsbackup-restore-test" : "false"
        }
      }
    },
    {
      "Sid" : "DdbDeleteActions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DeleteTable",
        "dynamodb:DescribeTable"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/awsbackup-restore-test-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RedshiftDeleteActions",
      "Effect" : "Allow",
      "Action" : "redshift:DeleteCluster",
      "Resource" : "arn:aws:redshift:*:*:cluster:awsbackup-restore-test-*"
    },
    {
      "Sid" : "S3DeleteActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration"
      ],
      "Resource" : "arn:aws:s3:::awsbackup-restore-test-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
```

```
      "Sid" : "TimestreamDeleteActions",
      "Effect" : "Allow",
      "Action" : "timestream:DeleteTable",
      "Resource" : "arn:aws:timestream:*:*:database/*/table/awsbackup-restore-test-*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSServiceRolePolicyForWorkspacesInstances

Deskripsi: Kebijakan terkelola ini menyediakan akses administratif WorkSpaces ke Amazon untuk mengelola EC2 instans di Akun AWS

`AWSServiceRolePolicyForWorkspacesInstances`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 11 Juni 2025, 20:37 UTC
- Waktu yang telah diedit: 11 Juni 2025, 20:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRolePolicyForWorkspacesInstances`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSShieldDRTAccessPolicy

Deskripsi: Menyediakan Tim Respons AWS DDo S dengan akses terbatas ke Anda Akun AWS untuk membantu mitigasi serangan DDo S selama peristiwa tingkat keparahan tinggi.

`AWSShieldDRTAccessPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSShieldDRTAccessPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 05 Juni 2018, 22:29 UTC
- Waktu yang telah diedit: 15 Desember 2020, 17:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSShieldDRTAccessPolicy`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SRTAccessProtectedResources",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:List*",
        "route53:List*",
        "elasticloadbalancing:Describe*",
        "cloudwatch:Describe*",
```

```
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "cloudfront:GetDistribution*",
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:DescribeAccelerator",
        "ec2:DescribeRegions",
        "ec2:DescribeAddresses"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SRTManageProtections",
      "Effect" : "Allow",
      "Action" : [
        "shield:*",
        "waf:*",
        "wafv2:*",
        "waf-regional:*",
        "elasticloadbalancing:SetWebACL",
        "cloudfront:UpdateDistribution",
        "apigateway:SetWebACL"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSShieldServiceRolePolicy

Deskripsi: Memungkinkan AWS Shield mengakses AWS sumber daya atas nama Anda untuk memberikan perlindungan DDo S.

`AWSShieldServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 17 November 2021 19:17 UTC
- Waktu yang telah diedit: 17 November 2021 19:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSShieldServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSShield",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:GetWebACL",
        "wafv2:UpdateWebACL",
        "wafv2:GetWebACLForResource",
        "wafv2:ListResourcesForWebACL",
        "cloudfront:ListDistributions",
        "cloudfront:GetDistribution"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSSocialMessagingServiceRolePolicy

Deskripsi: Menyediakan akses untuk mempublikasikan metrik dan memberikan wawasan untuk pengiriman pesan sosial Anda.

`AWSSocialMessagingServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 10 Oktober 2024, 19:28 UTC
- Waktu telah diedit: 10 Oktober 2024, 19:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSocialMessagingServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSSSMForSAPServiceLinkedRolePolicy

Deskripsi: Menyediakan AWS Systems Manager untuk SAP dengan izin yang diperlukan untuk mengelola dan mengintegrasikan perangkat lunak SAP dengan. AWS

`AWSSSMForSAPServiceLinkedRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan

- Waktu pembuatan: 16 November 2022, 01:18 UTC
- Waktu telah diedit: 08 Juli 2025, 23:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSSMForSAPServiceLinkedRolePolicy`

Versi kebijakan

Versi kebijakan: v12 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeInstanceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeRouteTables",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeVolumes",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeSnapshots",
        "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" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSSSMOpsInsightsServiceRolePolicy

Deskripsi: Kebijakan untuk Peran Tertaut Layanan AWSServiceRoleForAmazonSSM_OpsInsights

`AWSSSMOpsInsightsServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 16 Juni 2021 20:12 UTC
- Waktu yang telah diedit: 16 Juni 2021, 20:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSSMOpsInsightsServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCreateOpsItem",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateOpsItem",
        "ssm:AddTagsToResource"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "AllowAccessOpsItem",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateOpsItem",
        "ssm:GetOpsItem"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SsmOperationalInsight" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSSSODirectoryAdministrator

Deskripsi: Akses administrator untuk Direktori SSO

`AWSSSODirectoryAdministrator`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSSSODirectoryAdministrator` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 31 Oktober 2018, 23:54 UTC
- Waktu telah diedit: 20 Oktober 2022 20.34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSSODirectoryAdministrator`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSSODirectoryAdministrator",
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:*",
        "identitystore:*",
        "identitystore-auth:*",
        "sso:ListDirectoryAssociations"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSSSODirectoryReadOnly

Deskripsi: ReadOnly akses untuk Direktori SSO

`AWSSSODirectoryReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSSSODirectoryReadOnly` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 31 Oktober 2018, 23:49 UTC
- Waktu yang telah diedit: 16 November 2022, 18.17 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSSODirectoryReadOnly`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSSODirectoryReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:Search*",
        "sso-directory:Describe*",
        "sso-directory:List*",
        "sso-directory:Get*",
        "identitystore:Describe*",
        "identitystore:List*",
        "identitystore-auth:ListSessions",
        "identitystore-auth:BatchGetSession"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSSSOMasterAccountAdministrator

Deskripsi: Menyediakan akses dalam AWS SSO untuk mengelola akun master dan anggota AWS Organisasi dan aplikasi cloud

`AWSSSOMasterAccountAdministrator`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSSSOMasterAccountAdministrator` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Juni 2018, 20:36 UTC
- Waktu yang telah diedit: September 26, 2024, 17:13 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSSOMasterAccountAdministrator`

Versi kebijakan

Versi kebijakan: v10 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSSOCreateSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/
AWSServiceRoleForSSO",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "sso.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AWSSSOMasterAccountAdministrator",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/
AWSServiceRoleForSSO",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "sso.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AWSSSOMemberAccountAdministrator",
      "Effect" : "Allow",
      "Action" : [
        "ds:DescribeTrusts",
        "ds:UnauthorizeApplication",
        "ds:DescribeDirectories",
        "ds:AuthorizeApplication",
        "iam:ListPolicies",
        "organizations:EnableAWSServiceAccess",
        "organizations:ListRoots",
        "organizations:ListAccounts",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAccountsForParent",
```

```
        "organizations:DescribeOrganization",
        "organizations:ListChildren",
        "organizations:DescribeAccount",
        "organizations:ListParents",
        "organizations:ListDelegatedAdministrators",
        "sso:*",
        "sso-directory:*",
        "identitystore:*",
        "identitystore-auth:*",
        "ds:CreateAlias",
        "access-analyzer:ValidatePolicy",
        "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/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSSSOMemberAccountAdministrator

Deskripsi: Menyediakan akses dalam AWS SSO untuk mengelola akun anggota AWS Organizations dan aplikasi cloud

`AWSSSOMemberAccountAdministrator`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSSSOMemberAccountAdministrator` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Juni 2018, 20:45 UTC
- Waktu yang telah diedit: 26 April 2024, 00:31 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSSOMemberAccountAdministrator`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSSOMemberAccountAdministrator",
      "Effect" : "Allow",
      "Action" : [
        "ds:DescribeDirectories",
        "ds:AuthorizeApplication",
        "ds:UnauthorizeApplication",
        "ds:DescribeTrusts",
        "iam:ListPolicies",
        "organizations:EnableAWSServiceAccess",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "organizations:ListRoots",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListParents",
        "organizations:ListChildren",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListDelegatedAdministrators",
        "sso:*",
        "sso-directory:*",
        "identitystore:*",
        "identitystore-auth:*",
        "ds:CreateAlias",
        "access-analyzer:ValidatePolicy",
        "signin:CreateTrustedIdentityPropagationApplicationForConsole",
        "signin:ListTrustedIdentityPropagationApplicationsForConsole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSSSOManageDelegatedAdministrator",
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "sso.amazonaws.com"
        }
```

```
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSSSOReadOnly

Deskripsi: Menyediakan akses baca saja ke konfigurasi AWS SSO.

`AWSSSOReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSSSOReadOnly` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Juni 2018, 20:24 UTC
- Waktu yang telah diedit: 26 April 2024, 00:44 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSSOReadOnly`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSSOReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "ds:DescribeDirectories",
        "ds:DescribeTrusts",
        "iam:ListPolicies",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "organizations:ListParents",
        "organizations:ListChildren",
        "organizations:ListAccounts",
        "organizations:ListRoots",
        "organizations:ListAccountsForParent",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListDelegatedAdministrators",
        "sso:Describe*",
        "sso:Get*",
        "sso:List*",
        "sso:Search*",
        "sso-directory:DescribeDirectory",
        "access-analyzer:ValidatePolicy",
        "signin:ListTrustedIdentityPropagationApplicationsForConsole"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSSSOServiceRolePolicy

Deskripsi: Memberikan izin AWS SSO untuk mengelola AWS sumber daya, termasuk peran IAM, kebijakan, dan IDP SAMP atas nama Anda.

`AWSSSOServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 05 Desember 2017, 18:36 UTC
- Waktu yang telah diedit: 11 Februari 2025, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSSOServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v18 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IAMRoleProvisioningActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:CreateRole",
        "iam:PutRolePolicy",
```

```
        "iam:UpdateRole",
        "iam:UpdateRoleDescription",
        "iam:UpdateAssumeRolePolicy",
        "iam:PutRolePermissionsBoundary",
        "iam:DeleteRolePermissionsBoundary"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-reserved/sso.amazonaws.com/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalOrgMasterAccountId" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "IAMRoleReadActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRoles"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "IAMRoleCleanupActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-reserved/sso.amazonaws.com/*"
      ]
    },
    {
      "Sid" : "IAMSLRCleanupActions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus",
        "iam:DeleteRole",
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/AWSServiceRoleForSSO"
      ]
    },
    {
      "Sid" : "IAMSAMLProviderCreationAction",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateSAMLProvider"
      ],
      "Resource" : [
        "arn:aws:iam::*:saml-provider/AWSSSO_*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalOrgMasterAccountId" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "IAMSAMLProviderUpdateAction",
      "Effect" : "Allow",
      "Action" : [
        "iam:UpdateSAMLProvider"
      ],
      "Resource" : [
        "arn:aws:iam::*:saml-provider/AWSSSO_*"
      ]
    },
    {
      "Sid" : "IAMSAMLProviderCleanupActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteSAMLProvider",
        "iam:GetSAMLProvider"
      ],
      "Resource" : [
        "arn:aws:iam::*:saml-provider/AWSSSO_*"
      ]
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowUnauthAppForDirectory",
      "Effect" : "Allow",
      "Action" : [
        "ds:UnauthorizeApplication"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowDescribeForDirectory",
      "Effect" : "Allow",
      "Action" : [
        "ds:DescribeDirectories",
        "ds:DescribeTrusts"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowDescribeAndListOperationsOnIdentitySource",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeUser",
        "identitystore:DescribeGroup",
        "identitystore:ListGroups",
        "identitystore:ListUsers"
      ],
```

```
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowDeleteSyncProfile",
      "Effect" : "Allow",
      "Action" : [
        "identity-sync:DeleteSyncProfile"
      ],
      "Resource" : [
        "arn:aws:identity-sync:*:*:profile/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSStepFunctionsConsoleFullAccess

Deskripsi: Kebijakan akses untuk menyediakan user/role/etc akses ke AWS StepFunctions konsol. Untuk pengalaman konsol yang lengkap, selain kebijakan ini, pengguna mungkin memerlukan PassRole izin iam: pada peran IAM lain yang dapat diasumsikan oleh layanan.

`AWSStepFunctionsConsoleFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSStepFunctionsConsoleFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 11 Januari 2017, 21:54 UTC
- Waktu yang telah diedit: 12 Januari 2017, 00:19 UTC

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

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "states:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:ListRoles",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/service-role/StatesExecutionRole*"
    },
    {
      "Effect" : "Allow",
      "Action" : "lambda:ListFunctions",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSStepFunctionsFullAccess

Deskripsi: Kebijakan akses untuk menyediakan user/role/etc akses ke AWS StepFunctions API. Untuk akses penuh, selain kebijakan ini, pengguna HARUS memiliki PassRole izin iam: pada setidaknya satu peran IAM yang dapat diasumsikan oleh layanan.

`AWSStepFunctionsFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSStepFunctionsFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 11 Januari 2017, 21:51 UTC
- Waktu telah diedit: 11 Januari 2017, 21:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStepFunctionsFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      "Effect" : "Allow",
      "Action" : "states:*",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSStepFunctionsReadOnlyAccess

Deskripsi: Kebijakan akses untuk menyediakan akses hanya user/role/etc baca ke AWS StepFunctions layanan.

`AWSStepFunctionsReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSStepFunctionsReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 11 Januari 2017, 21:46 UTC
- Waktu yang telah diedit: 26 April 2024, 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStepFunctionsReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSStorageGatewayFullAccess

Deskripsi: Menyediakan akses penuh ke AWS Storage Gateway melalui file AWS Management Console.

`AWSStorageGatewayFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSStorageGatewayFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu yang telah diedit: 06 September 2022, 20.26 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStorageGatewayFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      "Action" : [
        "ec2:DescribeSnapshots",
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "fetchStorageGatewayParams",
      "Effect" : "Allow",
      "Action" : "ssm:GetParameters",
      "Resource" : "arn:aws:ssm:*::parameter/aws/service/storagegateway/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSStorageGatewayReadOnlyAccess

Deskripsi: Menyediakan akses ke AWS Storage Gateway melalui file AWS Management Console.

`AWSStorageGatewayReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSStorageGatewayReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu yang telah diedit: 06 September 2022, 20.24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStorageGatewayReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:List*",
        "storagegateway:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "fetchStorageGatewayParams",
      "Effect" : "Allow",
      "Action" : "ssm:GetParameters",
      "Resource" : "arn:aws:ssm:*::parameter/aws/service/storagegateway/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSStorageGatewayServiceRolePolicy

Deskripsi: Peran terkait layanan yang digunakan oleh AWS Storage Gateway untuk mengaktifkan integrasi AWS layanan lain dengan Storage Gateway.

`AWSStorageGatewayServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 17 Februari 2021, 19:03 UTC
- Waktu yang telah diedit: 17 Februari 2021, 19:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSStorageGatewayServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
    {
      "Effect" : "Allow",
      "Action" : [
        "fsx:ListTagsForResource"
      ],
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSSupplyChainFederationAdminAccess

Deskripsi: AWSSupply ChainFederationAdminAccess menyediakan akses pengguna federasi AWS Supply Chain ke aplikasi AWS Supply Chain, termasuk izin yang diperlukan untuk melakukan tindakan dalam aplikasi AWS Supply Chain. Kebijakan ini memberikan izin administratif atas pengguna dan grup IAM Identity Center dan dilampirkan ke peran yang dibuat oleh AWS Supply Chain atas nama Anda. Anda tidak boleh melampirkan AWSSupply ChainFederationAdminAccess kebijakan ke entitas IAM lainnya.

`AWSSupplyChainFederationAdminAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSSupplyChainFederationAdminAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 01 Maret 2023, 18:54 UTC
- Waktu yang telah diedit: 11 Desember 2024, 21:36 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSSupplyChainFederationAdminAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSupplyChain",
      "Effect" : "Allow",
      "Action" : [
        "scn:*"
      ],
      "Resource" : [
        "arn:aws:scn:*:*:instance/*"
      ]
    },
    {
      "Sid" : "ChimeAppInstance",
      "Effect" : "Allow",
      "Action" : [
        "chime:BatchCreateChannelMembership",
        "chime:CreateAppInstanceUser",
        "chime:CreateChannel",
        "chime:CreateChannelMembership",
        "chime:CreateChannelModerator",
        "chime:Connect",
        "chime:DeleteChannelMembership",
        "chime:DeleteChannelModerator",
        "chime:DescribeChannelMembershipForAppInstanceUser",
        "chime:GetChannelMembershipPreferences",
        "chime:ListChannelMemberships",
        "chime:ListChannelMembershipsForAppInstanceUser",
        "chime:ListChannelMessages",
        "chime:ListChannelModerators",
        "chime:TagResource",
        "chime:PutChannelMembershipPreferences",
```

```
        "chime:SendChannelMessage",
        "chime:UpdateChannelReadMarker",
        "chime:UpdateAppInstanceUser"
      ],
      "Resource" : [
        "arn:aws:chime:*:*:app-instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/SCNInstanceId" : "*"
        }
      }
    },
    {
      "Sid" : "ChimeChannel",
      "Effect" : "Allow",
      "Action" : [
        "chime:DescribeChannel"
      ],
      "Resource" : [
        "arn:aws:chime:*:*:app-instance/*"
      ]
    },
    {
      "Sid" : "ChimeMessaging",
      "Effect" : "Allow",
      "Action" : [
        "chime:GetMessagingSessionEndpoint"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
        "sso:GetManagedApplicationInstance",
        "sso:ListDirectoryAssociations",
        "sso:AssociateProfile",
        "sso:DisassociateProfile",
        "sso:ListProfiles",
        "sso:GetProfile",
        "sso:ListProfileAssociations",
        "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"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSSupportAccess

Deskripsi: Memungkinkan pengguna untuk mengakses AWS Dukungan Pusat.

`AWSSupportAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSSupportAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu telah diedit: 06 Februari 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSSupportAppFullAccess

Deskripsi: Menyediakan akses penuh ke AWS Dukungan Aplikasi dan layanan lain yang diperlukan, seperti AWS Dukungan dan Service Quotas. Kebijakan ini mencakup izin untuk menggunakan layanan pendukung sehingga pengguna dapat menghubungi AWS Dukungan untuk kasus dukungan, mengubah kuota layanan, dan membuat peran terkait layanan yang relevan.

`AWSSupportAppFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSSupportAppFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 22 Agustus 2022, 16:53 UTC
- Waktu yang telah diedit: 22 Agustus 2022, 16.53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportAppFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetRequestedServiceQuotaChange",
        "servicequotas:GetServiceQuota",
        "servicequotas:RequestServiceQuotaIncrease",
```

```
        "support:AddAttachmentsToSet",
        "support:AddCommunicationToCase",
        "support:CreateCase",
        "support:DescribeCases",
        "support:DescribeCommunications",
        "support:DescribeSeverityLevels",
        "support:InitiateChatForCase",
        "support:ResolveCase"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "servicequotas.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSSupportAppReadOnlyAccess

Deskripsi: Menyediakan akses hanya-baca ke Aplikasi. AWS Dukungan

`AWSSupportAppReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSSupportAppReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 22 Agustus 2022, 17:01 UTC
- Waktu yang telah diedit: 22 Agustus 2022, 17.01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportAppReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSSupportPlansFullAccess

Deskripsi: Menyediakan akses penuh ke supportplans.

`AWSSupportPlansFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSSupportPlansFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 September 2022, 18:19 UTC
- Waktu yang telah diedit: 09 September 2024, 21:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportPlansFullAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "supportplans:GetSupportPlan",
        "supportplans:GetSupportPlanUpdateStatus",
        "supportplans:ListSupportPlanModifiers",
        "supportplans:StartSupportPlanUpdate",
        "supportplans:CreateSupportPlanSchedule"
      ],
```

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSSupportPlansReadOnlyAccess

Deskripsi: Menyediakan akses hanya-baca ke supportplan.

`AWSSupportPlansReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSSupportPlansReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 September 2022, 18.08 UTC
- Waktu yang telah diedit: 09 September 2024, 21:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportPlansReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


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


Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSSupportServiceRolePolicy

Deskripsi: Memungkinkan AWS Dukungan untuk mengakses AWS sumber daya untuk menyediakan layanan penagihan, administrasi, dan dukungan.

`AWSSupportServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 19 April 2018, 18:04 UTC
- Waktu yang telah diedit: 18 Juni 2025, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSupportServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v40 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Statement" : [
    {
      "Sid" : "AWSSupportAPIGatewayAccess",
      "Action" : [
        "apigateway:GET"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:apigateway:*::/account",
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/apis/*/authorizers",
        "arn:aws:apigateway:*::/apis/*/authorizers/*",
        "arn:aws:apigateway:*::/apis/*/deployments",
        "arn:aws:apigateway:*::/apis/*/deployments/*",
        "arn:aws:apigateway:*::/apis/*/integrations",
        "arn:aws:apigateway:*::/apis/*/integrations/*",
        "arn:aws:apigateway:*::/apis/*/integrations/*/integrationresponses",
        "arn:aws:apigateway:*::/apis/*/integrations/*/integrationresponses/*",
        "arn:aws:apigateway:*::/apis/*/models",
        "arn:aws:apigateway:*::/apis/*/models/*",
        "arn:aws:apigateway:*::/apis/*/routes",
```

```
        "arn:aws:apigateway:*::/apis/*/routes/*",
        "arn:aws:apigateway:*::/apis/*/routes/*/routeresponses",
        "arn:aws:apigateway:*::/apis/*/routes/*/routeresponses/*",
        "arn:aws:apigateway:*::/apis/*/stages",
        "arn:aws:apigateway:*::/apis/*/stages/*",
        "arn:aws:apigateway:*::/clientcertificates",
        "arn:aws:apigateway:*::/clientcertificates/*",
        "arn:aws:apigateway:*::/domainnames",
        "arn:aws:apigateway:*::/domainnames/*",
        "arn:aws:apigateway:*::/domainnames/*/apimappings",
        "arn:aws:apigateway:*::/domainnames/*/apimappings/*",
        "arn:aws:apigateway:*::/domainnames/*/basepathmappings",
        "arn:aws:apigateway:*::/domainnames/*/basepathmappings/*",
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/restapis/*/authorizers",
        "arn:aws:apigateway:*::/restapis/*/authorizers/*",
        "arn:aws:apigateway:*::/restapis/*/deployments",
        "arn:aws:apigateway:*::/restapis/*/deployments/*",
        "arn:aws:apigateway:*::/restapis/*/models",
        "arn:aws:apigateway:*::/restapis/*/models/*",
        "arn:aws:apigateway:*::/restapis/*/models/*/default_template",
        "arn:aws:apigateway:*::/restapis/*/resources",
        "arn:aws:apigateway:*::/restapis/*/resources/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integration/responses/
*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/responses/*",
        "arn:aws:apigateway:*::/restapis/*/stages/*/sdks/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integration",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/usageplans",
        "arn:aws:apigateway:*::/usageplans/*",
        "arn:aws:apigateway:*::/vpclinks",
        "arn:aws:apigateway:*::/vpclinks/*"
      ]
    },
    {
      "Sid" : "AWSSupportDeleteRoleAccess",
      "Action" : [
        "iam:DeleteRole"
      ],
      "Effect" : "Allow",
```

```
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/support.amazonaws.com/
AWSServiceRoleForSupport"
      ]
    },
    {
      "Sid" : "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",
        "airflow:getEnvironment",
        "airflow:listEnvironments",
        "airflow:listTagsForResource",
        "amplify:getApp",
        "amplify:getBackendEnvironment",
        "amplify:getBranch",
        "amplify:getDomainAssociation",
        "amplify:getJob",
        "amplify:getWebhook",
```

```
        "amplify:listApps",
        "amplify:listBackendEnvironments",
        "amplify:listBranches",
        "amplify:listDomainAssociations",
        "amplify:listWebhooks",
        "amplifyuibuilder:exportComponents",
        "amplifyuibuilder:exportThemes",
        "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:getApi",
        "appsync:getApiAssociation",
        "appsync:getApiCache",
        "appsync:getChannelNamespace",
        "appsync:getDataSource",
        "appsync:getDomainName",
        "appsync:getFunction",
        "appsync:getGraphqlApi",
        "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: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:listBackupPlans",
        "backup:listBackupPlanTemplates",
        "backup:listBackupPlanVersions",
        "backup:listBackupSelections",
        "backup:listBackupVaults",
        "backup:listCopyJobs",
        "backup:listFrameworks",
        "backup:listLegalHolds",
        "backup:listProtectedResources",
        "backup:listRecoveryPointsByBackupVault",
        "backup:listRecoveryPointsByLegalHold",
        "backup:listRecoveryPointsByResource",
        "backup:listReportJobs",
        "backup:listReportPlans",
        "backup:listRestoreJobs",
        "backup:listRestoreJobsByProtectedResource",
        "backup:listRestoreTestingPlans",
        "backup:listRestoreTestingSelections",
        "backup:listTags",
        "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:getConfiguredTable",
        "cleanrooms:getConfiguredTableAssociation",
        "cleanrooms:getMembership",
        "cleanrooms:getSchema",
        "cleanrooms:listAnalysisTemplates",
        "cleanrooms:listCollaborationAnalysisTemplates",
        "cleanrooms:listCollaborations",
        "cleanrooms:listConfiguredTableAssociations",
        "cleanrooms:listConfiguredTables",
        "cleanrooms:listMembers",
        "cleanrooms:listMemberships",
        "cleanrooms:listSchemas",
        "cloud9:describeEnvironmentMemberships",
        "cloud9:describeEnvironments",
        "cloud9:listEnvironments",
        "clouddirectory:getDirectory",
        "clouddirectory:listDirectories",
        "cloudformation:batchDescribeTypeConfigurations",
        "cloudformation:describeAccountLimits",
        "cloudformation:describeChangeSet",
        "cloudformation:describeChangeSetHooks",
        "cloudformation:describePublisher",
        "cloudformation:describeStackEvents",
        "cloudformation:describeStackInstance",
        "cloudformation:describeStackResource",
        "cloudformation:describeStackResources",
        "cloudformation:describeStacks",
        "cloudformation:describeStackSet",
        "cloudformation:describeStackSetOperation",
        "cloudformation:describeType",
        "cloudformation:describeTypeRegistration",
```

```
        "cloudformation:estimateTemplateCost",
        "cloudformation:getStackPolicy",
        "cloudformation:getTemplate",
        "cloudformation:getTemplateSummary",
        "cloudformation:listChangeSets",
        "cloudformation:listExports",
        "cloudformation:listImports",
        "cloudformation:listStackInstances",
        "cloudformation:listStackResources",
        "cloudformation:listStacks",
        "cloudformation:listStackSetOperationResults",
        "cloudformation:listStackSetOperations",
        "cloudformation:listStackSets",
        "cloudformation:listTypeRegistrations",
        "cloudformation:listTypes",
        "cloudformation:listTypeVersions",
        "cloudfront:describeFunction",
        "cloudfront: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:describeIdentityPool",
        "cognito-identity:getIdentityPoolRoles",
        "cognito-identity:listIdentities",
        "cognito-identity:listIdentityPools",
        "cognito-idp:describeIdentityProvider",
        "cognito-idp:describeResourceServer",
        "cognito-idp:describeRiskConfiguration",
        "cognito-idp:describeUserImportJob",
        "cognito-idp:describeUserPool",
        "cognito-idp:describeUserPoolClient",
        "cognito-idp:describeUserPoolDomain",
        "cognito-idp:getGroup",
        "cognito-idp:getUICustomization",
        "cognito-idp:getUserPoolMfaConfig",
        "cognito-idp:listGroups",
        "cognito-idp:listIdentityProviders",
        "cognito-idp:listResourceServers",
        "cognito-idp:listUserImportJobs",
        "cognito-idp:listUserPoolClients",
        "cognito-idp:listUserPools",
        "cognito-sync:describeDataset",
        "cognito-sync:describeIdentityPoolUsage",
        "cognito-sync:describeIdentityUsage",
        "cognito-sync:getCognitoEvents",
        "cognito-sync:getIdentityPoolConfiguration",
        "cognito-sync:listDatasets",
        "cognito-sync:listIdentityPoolUsage",
        "comprehend:describeDocumentClassificationJob",
        "comprehend:describeDocumentClassifier",
        "comprehend:describeDominantLanguageDetectionJob",
        "comprehend:describeEndpoint",
        "comprehend:describeEntitiesDetectionJob",
```

```
        "comprehend:describeEntityRecognizer",
        "comprehend:describeEventsDetectionJob",
        "comprehend:describeFlywheel",
        "comprehend:describeFlywheelIteration",
        "comprehend:describeKeyPhrasesDetectionJob",
        "comprehend:describePiiEntitiesDetectionJob",
        "comprehend:describeSentimentDetectionJob",
        "comprehend:describeTargetedSentimentDetectionJob",
        "comprehend:describeTopicsDetectionJob",
        "comprehend:listDocumentClassificationJobs",
        "comprehend:listDocumentClassifiers",
        "comprehend:listDominantLanguageDetectionJobs",
        "comprehend:listEndpoints",
        "comprehend:listEntitiesDetectionJobs",
        "comprehend:listEntityRecognizers",
        "comprehend:listEventsDetectionJobs",
        "comprehend:listFlywheelIterationHistory",
        "comprehend:listFlywheels",
        "comprehend:listKeyPhrasesDetectionJobs",
        "comprehend:listPiiEntitiesDetectionJobs",
        "comprehend:listSentimentDetectionJobs",
        "comprehend:listTargetedSentimentDetectionJobs",
        "comprehend:listTopicsDetectionJobs",
        "compute-optimizer:getAutoScalingGroupRecommendations",
        "compute-optimizer:getEBSVolumeRecommendations",
        "compute-optimizer:getEC2InstanceRecommendations",
        "compute-optimizer:getEC2RecommendationProjectedMetrics",
        "compute-optimizer:getECSServiceRecommendationProjectedMetrics",
        "compute-optimizer:getECSServiceRecommendations",
        "compute-optimizer:getEnrollmentStatus",
        "compute-optimizer:getRecommendationSummaries",
        "config:batchGetAggregateResourceConfig",
        "config:batchGetResourceConfig",
        "config:describeAggregateComplianceByConfigRules",
        "config:describeAggregationAuthorizations",
        "config:describeComplianceByConfigRule",
        "config:describeComplianceByResource",
        "config:describeConfigRuleEvaluationStatus",
        "config:describeConfigRules",
        "config:describeConfigurationAggregators",
        "config:describeConfigurationAggregatorSourcesStatus",
        "config:describeConfigurationRecorders",
        "config:describeConfigurationRecorderStatus",
        "config:describeConformancePackCompliance",
```

```
        "config:describeConformancePacks",
        "config:describeConformancePackStatus",
        "config:describeDeliveryChannels",
        "config:describeDeliveryChannelStatus",
        "config:describeOrganizationConfigRules",
        "config:describeOrganizationConfigRuleStatuses",
        "config:describeOrganizationConformancePacks",
        "config:describeOrganizationConformancePackStatuses",
        "config:describePendingAggregationRequests",
        "config:describeRemediationConfigurations",
        "config:describeRemediationExceptions",
        "config:describeRemediationExecutionStatus",
        "config:describeRetentionConfigurations",
        "config:getAggregateComplianceDetailsByConfigRule",
        "config:getAggregateConfigRuleComplianceSummary",
        "config:getAggregateDiscoveredResourceCounts",
        "config:getAggregateResourceConfig",
        "config:getComplianceDetailsByConfigRule",
        "config:getComplianceDetailsByResource",
        "config:getComplianceSummaryByConfigRule",
        "config:getComplianceSummaryByResourceType",
        "config:getConformancePackComplianceDetails",
        "config:getConformancePackComplianceSummary",
        "config:getDiscoveredResourceCounts",
        "config:getOrganizationConfigRuleDetailedStatus",
        "config:getOrganizationConformancePackDetailedStatus",
        "config:getResourceConfigHistory",
        "config:listAggregateDiscoveredResources",
        "config:listDiscoveredResources",
        "config:listTagsForResource",
        "config:selectResourceConfig",
        "connect:describeContact",
        "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: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:describeLDAPSSettings",
        "ds:describeSharedDirectories",
        "ds:describeSnapshots",
        "ds:describeTrusts",
        "ds:getDirectoryLimits",
        "ds:getSnapshotLimits",
        "ds:listIpRoutes",
        "ds:listSchemaExtensions",
        "ds:listTagsForResource",
        "dynamodb:describeBackup",
        "dynamodb:describeContinuousBackups",
        "dynamodb:describeContributorInsights",
        "dynamodb:describeExport",
        "dynamodb:describeGlobalTable",
        "dynamodb:describeImport",
        "dynamodb:describeKinesisStreamingDestination",
        "dynamodb:describeLimits",
        "dynamodb:describeStream",
        "dynamodb:describeTable",
        "dynamodb:describeTimeToLive",
        "dynamodb: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: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:describeReleaseLabel",
        "elasticmapreduce:describeSecurityConfiguration",
        "elasticmapreduce:describeStep",
        "elasticmapreduce:describeStudio",
        "elasticmapreduce:getAutoTerminationPolicy",
        "elasticmapreduce:getBlockPublicAccessConfiguration",
        "elasticmapreduce:getManagedScalingPolicy",
        "elasticmapreduce:getStudioSessionMapping",
        "elasticmapreduce:listBootstrapActions",
        "elasticmapreduce:listClusters",
        "elasticmapreduce:listInstanceFleets",
        "elasticmapreduce:listInstanceGroups",
        "elasticmapreduce:listInstances",
        "elasticmapreduce:listNotebookExecutions",
        "elasticmapreduce:listReleaseLabels",
        "elasticmapreduce:listSecurityConfigurations",
        "elasticmapreduce:listSteps",
        "elasticmapreduce:listStudios",
```

```
        "elasticmapreduce:listStudioSessionMappings",
        "elastictranscoder:listJobsByPipeline",
        "elastictranscoder:listJobsByStatus",
        "elastictranscoder:listPipelines",
        "elastictranscoder:listPresets",
        "elastictranscoder:readPipeline",
        "elastictranscoder:readPreset",
        "emr-containers:describeJobRun",
        "emr-containers:describeJobTemplate",
        "emr-containers:describeManagedEndpoint",
        "emr-containers:describeVirtualCluster",
        "emr-containers:listJobRuns",
        "emr-containers:listJobTemplates",
        "emr-containers:listManagedEndpoints",
        "emr-containers:listVirtualClusters",
        "emr-serverless:getApplication",
        "emr-serverless:getJobRun",
        "emr-serverless:listApplications",
        "es:describeDomain",
        "es:describeDomainAutoTunes",
        "es:describeDomainChangeProgress",
        "es:describeDomainConfig",
        "es:describeDomains",
        "es:describeDryRunProgress",
        "es:describeElasticsearchDomain",
        "es:describeElasticsearchDomainConfig",
        "es:describeElasticsearchDomains",
        "es:describeInboundConnections",
        "es:describeInstanceTypeLimits",
        "es:describeOutboundConnections",
        "es:describePackages",
        "es:describeReservedInstanceOfferings",
        "es:describeReservedInstances",
        "es:describeVpcEndpoints",
        "es:getCompatibleVersions",
        "es:getPackageVersionHistory",
        "es:getUpgradeHistory",
        "es:getUpgradeStatus",
        "es:listDomainNames",
        "es:listDomainsForPackage",
        "es:listInstanceTypeDetails",
        "es:listPackagesForDomain",
        "es:listScheduledActions",
        "es:listTags",
```

```
        "es:listVersions",
        "es:listVpcEndpointAccess",
        "es:listVpcEndpoints",
        "es:listVpcEndpointsForDomain",
        "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:getExperiment",
        "fis:getExperimentTemplate",
        "fis:listExperiments",
        "fis:listExperimentTemplates",
        "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:describeSnapshots",
        "fsx:describeStorageVirtualMachines",
        "fsx:describeVolumes",
        "fsx:listTagsForResource",
```

```
        "gamelift:describeAlias",
        "gamelift:describeBuild",
        "gamelift:describeEC2InstanceLimits",
        "gamelift:describeFleetAttributes",
        "gamelift:describeFleetCapacity",
        "gamelift:describeFleetEvents",
        "gamelift:describeFleetLocationAttributes",
        "gamelift:describeFleetLocationCapacity",
        "gamelift:describeFleetLocationUtilization",
        "gamelift:describeFleetPortSettings",
        "gamelift:describeFleetUtilization",
        "gamelift:describeGameServer",
        "gamelift:describeGameServerGroup",
        "gamelift:describeGameSessionDetails",
        "gamelift:describeGameSessionPlacement",
        "gamelift:describeGameSessionQueues",
        "gamelift:describeGameSessions",
        "gamelift:describeInstances",
        "gamelift:describeMatchmaking",
        "gamelift:describeMatchmakingConfigurations",
        "gamelift:describeMatchmakingRuleSets",
        "gamelift:describePlayerSessions",
        "gamelift:describeRuntimeConfiguration",
        "gamelift:describeScalingPolicies",
        "gamelift:describeScript",
        "gamelift:listAliases",
        "gamelift:listBuilds",
        "gamelift:listFleets",
        "gamelift:listGameServerGroups",
        "gamelift:listGameServers",
        "gamelift:listScripts",
        "gamelift:resolveAlias",
        "glacier:describeJob",
        "glacier:describeVault",
        "glacier:getDataRetrievalPolicy",
        "glacier:getVaultAccessPolicy",
        "glacier:getVaultLock",
        "glacier:getVaultNotifications",
        "glacier:listJobs",
        "glacier:listTagsForVault",
        "glacier:listVaults",
        "globalaccelerator:describeAccelerator",
        "globalaccelerator:describeAcceleratorAttributes",
        "globalaccelerator:describeEndpointGroup",
```

```
        "globalaccelerator:describeListener",
        "globalaccelerator:listAccelerators",
        "globalaccelerator:listEndpointGroups",
        "globalaccelerator:listListeners",
        "glue:batchGetBlueprints",
        "glue:batchGetCrawlers",
        "glue:batchGetDevEndpoints",
        "glue:batchGetJobs",
        "glue:batchGetPartition",
        "glue:batchGetTriggers",
        "glue:batchGetWorkflows",
        "glue:checkSchemaVersionValidity",
        "glue:getBlueprint",
        "glue:getBlueprintRun",
        "glue:getBlueprintRuns",
        "glue:getCatalogImportStatus",
        "glue:getClassifier",
        "glue:getClassifiers",
        "glue:getColumnStatisticsForPartition",
        "glue:getColumnStatisticsForTable",
        "glue:getCrawler",
        "glue:getCrawlerMetrics",
        "glue:getCrawlers",
        "glue:getCustomEntityType",
        "glue:getDatabase",
        "glue:getDatabases",
        "glue:getDataflowGraph",
        "glue:getDataQualityResult",
        "glue:getDataQualityRuleRecommendationRun",
        "glue:getDataQualityRuleset",
        "glue:getDataQualityRulesetEvaluationRun",
        "glue:getDevEndpoint",
        "glue:getDevEndpoints",
        "glue:getJob",
        "glue:getJobRun",
        "glue:getJobRuns",
        "glue:getJobs",
        "glue:getMapping",
        "glue:getMLTaskRun",
        "glue:getMLTaskRuns",
        "glue:getMLTransform",
        "glue:getMLTransforms",
        "glue:getPartition",
        "glue:getPartitionIndexes",
```

```
        "glue:getPartitions",
        "glue:getRegistry",
        "glue:getResourcePolicies",
        "glue:getResourcePolicy",
        "glue:getSchema",
        "glue:getSchemaByDefinition",
        "glue:getSchemaVersion",
        "glue:getSchemaVersionsDiff",
        "glue:getSecurityConfiguration",
        "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: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:querySchemaVersionMetadata",
        "grafana:describeWorkspace",
        "grafana:describeWorkspaceAuthentication",
        "grafana:listPermissions",
        "grafana:listVersions",
        "grafana:listWorkspaces",
        "greengrass:getConnectivityInfo",
        "greengrass:getCoreDefinition",
```

```
        "greengrass:getCoreDefinitionVersion",
        "greengrass:getDeploymentStatus",
        "greengrass:getDeviceDefinition",
        "greengrass:getDeviceDefinitionVersion",
        "greengrass:getFunctionDefinition",
        "greengrass:getFunctionDefinitionVersion",
        "greengrass:getGroup",
        "greengrass:getGroupCertificateAuthority",
        "greengrass:getGroupVersion",
        "greengrass:getLoggerDefinition",
        "greengrass:getLoggerDefinitionVersion",
        "greengrass:getResourceDefinitionVersion",
        "greengrass:getServiceRoleForAccount",
        "greengrass:getSubscriptionDefinition",
        "greengrass:getSubscriptionDefinitionVersion",
        "greengrass:listCoreDefinitions",
        "greengrass:listCoreDefinitionVersions",
        "greengrass:listDeployments",
        "greengrass:listDeviceDefinitions",
        "greengrass:listDeviceDefinitionVersions",
        "greengrass:listFunctionDefinitions",
        "greengrass:listFunctionDefinitionVersions",
        "greengrass:listGroups",
        "greengrass:listGroupVersions",
        "greengrass:listLoggerDefinitions",
        "greengrass:listLoggerDefinitionVersions",
        "greengrass:listResourceDefinitions",
        "greengrass:listResourceDefinitionVersions",
        "greengrass:listSubscriptionDefinitions",
        "greengrass:listSubscriptionDefinitionVersions",
        "guardduty:describeMalwareScans",
        "guardduty:describePublishingDestination",
        "guardduty:getCoverageStatistics",
        "guardduty:getDetector",
        "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:listFindings",
        "guardduty:listInvitations",
        "guardduty:listIPSets",
        "guardduty:listMembers",
        "guardduty:listThreatIntelSets",
        "health:describeAffectedAccountsForOrganization",
        "health:describeAffectedEntities",
        "health:describeAffectedEntitiesForOrganization",
        "health:describeEntityAggregates",
        "health:describeEntityAggregatesForOrganization",
        "health:describeEventAggregates",
        "health:describeEventDetails",
        "health:describeEventDetailsForOrganization",
        "health:describeEvents",
        "health:describeEventsForOrganization",
        "health:describeEventTypes",
        "health:describeHealthServiceStatusForOrganization",
        "iam:getAccessKeyLastUsed",
        "iam:getAccountAuthorizationDetails",
        "iam:getAccountPasswordPolicy",
        "iam:getAccountSummary",
        "iam:getContextKeysForCustomPolicy",
        "iam:getContextKeysForPrincipalPolicy",
        "iam:getCredentialReport",
        "iam:getGroup",
        "iam:getGroupPolicy",
        "iam:getInstanceProfile",
        "iam:getLoginProfile",
        "iam:getOpenIDConnectProvider",
        "iam:getPolicy",
        "iam:getPolicyVersion",
        "iam:getRole",
        "iam:getRolePolicy",
        "iam:getSAMLProvider",
        "iam:getServerCertificate",
        "iam:getServiceLinkedRoleDeletionStatus",
        "iam:getSSHPublicKey",
        "iam:getUser",
        "iam:getUserPolicy",
        "iam:listAccessKeys",
        "iam:listAccountAliases",
```

```
        "iam:listAttachedGroupPolicies",
        "iam:listAttachedRolePolicies",
        "iam:listAttachedUserPolicies",
        "iam:listEntitiesForPolicy",
        "iam:listGroupPolicies",
        "iam:listGroups",
        "iam:listGroupsForUser",
        "iam:listInstanceProfiles",
        "iam:listInstanceProfilesForRole",
        "iam:listMFADevices",
        "iam:listOpenIDConnectProviders",
        "iam:listPolicies",
        "iam:listPolicyVersions",
        "iam:listRolePolicies",
        "iam:listRoles",
        "iam:listSAMLProviders",
        "iam:listServerCertificates",
        "iam:listSigningCertificates",
        "iam:listSSHPublicKeys",
        "iam:listUserPolicies",
        "iam:listUsers",
        "iam:listVirtualMFADevices",
        "iam:simulateCustomPolicy",
        "iam:simulatePrincipalPolicy",
        "imagebuilder:getComponent",
        "imagebuilder:getComponentPolicy",
        "imagebuilder:getContainerRecipe",
        "imagebuilder: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",
        "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",
        "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",
        "mq:describeBroker",
        "mq:describeConfiguration",
        "mq:describeConfigurationRevision",
        "mq:describeUser",
        "mq:listBrokers",
        "mq:listConfigurationRevisions",
        "mq:listConfigurations",
        "mq:listUsers",
        "network-firewall:describeFirewall",
        "network-firewall:describeFirewallPolicy",
        "network-firewall:describeLoggingConfiguration",
        "network-firewall:describeRuleGroup",
        "network-firewall:describeTlsInspectionConfiguration",
        "network-firewall:listFirewallPolicies",
        "network-firewall:listFirewalls",
        "network-firewall:listRuleGroups",
        "network-firewall:listTlsInspectionConfigurations",
        "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",
        "omics:getAnnotationImportJob",
        "omics:getAnnotationStore",
        "omics:getReadSetImportJob",
        "omics:getReadSetMetadata",
        "omics:getReference",
        "omics:getReferenceImportJob",
        "omics:getReferenceMetadata",
        "omics:getReferenceStore",
        "omics:getRun",
        "omics:getRunGroup",
        "omics:getSequenceStore",
        "omics:getVariantImportJob",
        "omics:getVariantStore",
        "omics:getWorkflow",
        "omics:listAnnotationImportJobs",
        "omics:listAnnotationStores",
        "omics:listMultipartReadSetUploads",
        "omics:listReadSetImportJobs",
        "omics:listReadSets",
        "omics:listReadSetUploadParts",
        "omics:listReferenceImportJobs",
        "omics:listReferences",
        "omics:listReferenceStores",
        "omics:listRunGroups",
        "omics:listRuns",
        "omics:listRunTasks",
        "omics:listSequenceStores",
        "omics:listVariantImportJobs",
        "omics:listVariantStores",
        "omics:listWorkflows",
        "opsworks-cm:describeAccountAttributes",
        "opsworks-cm:describeBackups",
        "opsworks-cm:describeEvents",
        "opsworks-cm:describeNodeAssociationStatus",
        "opsworks-cm:describeServers",
        "opsworks:describeAgentVersions",
        "opsworks:describeApps",
        "opsworks:describeCommands",
        "opsworks:describeDeployments",
```

```
        "opsworks:describeEcsClusters",
        "opsworks:describeElasticIps",
        "opsworks:describeElasticLoadBalancers",
        "opsworks:describeInstances",
        "opsworks:describeLayers",
        "opsworks:describeLoadBasedAutoScaling",
        "opsworks:describeMyUserProfile",
        "opsworks:describePermissions",
        "opsworks:describeRaidArrays",
        "opsworks:describeRdsDbInstances",
        "opsworks:describeServiceErrors",
        "opsworks:describeStackProvisioningParameters",
        "opsworks:describeStacks",
        "opsworks:describeStackSummary",
        "opsworks:describeTimeBasedAutoScaling",
        "opsworks:describeUserProfiles",
        "opsworks:describeVolumes",
        "opsworks:getHostnameSuggestion",
        "organizations:describeAccount",
        "organizations:describeCreateAccountStatus",
        "organizations:describeEffectivePolicy",
        "organizations:describeHandshake",
        "organizations:describeOrganization",
        "organizations:describePolicy",
        "organizations:describeResourcePolicy",
        "organizations:listAccounts",
        "organizations:listAWSServiceAccessForOrganization",
        "organizations:listCreateAccountStatus",
        "organizations:listDelegatedAdministrators",
        "organizations:listDelegatedServicesForAccount",
        "organizations:listHandshakesForAccount",
        "organizations:listHandshakesForOrganization",
        "organizations:listPoliciesForTarget",
        "organizations:listTagsForResource",
        "organizations:listTargetsForPolicy",
        "osis:getPipeline",
        "osis:getPipelineBlueprint",
        "osis:getPipelineChangeProgress",
        "osis:listPipelineBlueprints",
        "osis:listPipelines",
        "osis:validatePipeline",
        "outposts:getCatalogItem",
        "outposts:getConnection",
        "outposts:getOrder",
```

```
        "outposts:getOutpost",
        "outposts:getOutpostInstanceTypes",
        "outposts:getSite",
        "outposts:listAssets",
        "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: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:getTableBucketMaintenanceConfiguration",
        "s3tables:getTableBucketPolicy",
        "s3tables:getTableMaintenanceJobStatus",
        "s3tables:getTableMetadataLocation",
        "s3tables:getTablePolicy",
        "s3tables:listNamespaces",
        "s3tables:listTableBuckets",
        "s3tables:listTables",
        "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: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: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:batchGetConfigurationPolicyAssociations",
        "securityhub:describeOrganizationConfiguration",
        "securityhub:getConfigurationPolicy",
        "securityhub:getConfigurationPolicyAssociation",
        "securityhub:getEnabledStandards",
        "securityhub:getFindingAggregator",
        "securityhub:getFindings",
        "securityhub:getInsightResults",
        "securityhub:getInsights",
        "securityhub:getMasterAccount",
        "securityhub:getMembers",
        "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:describeActiveReceiptRuleSet",
        "ses:describeConfigurationSet",
        "ses:describeReceiptRule",
        "ses:describeReceiptRuleSet",
        "ses:getAccount",
        "ses:getAccountSendingEnabled",
        "ses:getBlacklistReports",
        "ses:getConfigurationSet",
        "ses:getConfigurationSetEventDestinations",
        "ses:getContactList",
        "ses:getDedicatedIp",
        "ses:getDedicatedIpPool",
```

```
        "ses:getDedicatedIps",
        "ses:getDeliverabilityDashboardOptions",
        "ses:getDeliverabilityTestReport",
        "ses:getDomainDeliverabilityCampaign",
        "ses:getDomainStatisticsReport",
        "ses:getEmailIdentity",
        "ses:getIdentityDkimAttributes",
        "ses:getIdentityMailFromDomainAttributes",
        "ses:getIdentityNotificationAttributes",
        "ses:getIdentityPolicies",
        "ses:getIdentityVerificationAttributes",
        "ses:getImportJob",
        "ses:getSendQuota",
        "ses:getSendStatistics",
        "ses:listConfigurationSets",
        "ses:listContactLists",
        "ses:listContacts",
        "ses:listCustomVerificationEmailTemplates",
        "ses:listDedicatedIpPools",
        "ses:listDeliverabilityTestReports",
        "ses:listDomainDeliverabilityCampaigns",
        "ses:listEmailIdentities",
        "ses:listEmailTemplates",
        "ses:listIdentities",
        "ses:listIdentityPolicies",
        "ses:listImportJobs",
        "ses:listReceiptFilters",
        "ses:listReceiptRuleSets",
        "ses:listRecommendations",
        "ses:listTagsForResource",
        "ses:listTemplates",
        "ses:listVerifiedEmailAddresses",
        "shield:describeAttack",
        "shield:describeProtection",
        "shield:describeSubscription",
        "shield:listAttacks",
        "shield:listProtections",
        "sms-voice:getConfigurationSetEventDestinations",
        "sms:getConnectors",
        "sms:getReplicationJobs",
        "sms:getReplicationRuns",
        "sms:getServers",
        "snowball:describeAddress",
        "snowball:describeAddresses",
```

```
        "snowball:describeJob",
        "snowball:getSnowballUsage",
        "snowball:listJobs",
        "snowball:listServiceVersions",
        "sns:checkIfPhoneNumberIsOptedOut",
        "sns:getDataProtectionPolicy",
        "sns:getEndpointAttributes",
        "sns:getPlatformApplicationAttributes",
        "sns:getSMSAttributes",
        "sns:getSMSSandboxAccountStatus",
        "sns:getSubscriptionAttributes",
        "sns:getTopicAttributes",
        "sns:listEndpointsByPlatformApplication",
        "sns:listOriginationNumbers",
        "sns:listPhoneNumbersOptedOut",
        "sns:listPlatformApplications",
        "sns:listSMSSandboxPhoneNumbers",
        "sns:listSubscriptions",
        "sns:listSubscriptionsByTopic",
        "sns:listTopics",
        "sqs:getQueueAttributes",
        "sqs:getQueueUrl",
        "sqs:listDeadLetterSourceQueues",
        "sqs: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:describeInstance",
        "sso:describeTrustedTokenIssuer",
        "sso:getApplicationAccessScope",
        "sso:getApplicationAssignmentConfiguration",
        "sso:getApplicationAuthenticationMethod",
        "sso:getApplicationGrant",
        "sso:getApplicationInstance",
        "sso:getApplicationTemplate",
        "sso:getManagedApplicationInstance",
        "sso:getSharedSsoConfiguration",
        "sso:listApplicationAccessScopes",
        "sso:listApplicationAssignments",
        "sso:listApplicationAuthenticationMethods",
        "sso:listApplicationGrants",
        "sso:listApplicationInstances",
        "sso:listApplicationProviders",
        "sso:listApplications",
        "sso:listApplicationTemplates",
        "sso:listDirectoryAssociations",
        "sso:listInstances",
        "sso:listProfileAssociations",
        "sso:listTrustedTokenIssuers",
        "states:describeActivity",
        "states:describeExecution",
        "states:describeMapRun",
        "states:describeStateMachine",
        "states:describeStateMachineAlias",
        "states:describeStateMachineForExecution",
        "states:getExecutionHistory",
        "states:listActivities",
        "states:listExecutions",
        "states:listMapRuns",
        "states:listStateMachineAliases",
        "states:listStateMachines",
```

```
        "states:listStateMachineVersions",
        "storagegateway:describeBandwidthRateLimit",
        "storagegateway:describeCache",
        "storagegateway:describeCachediSCSIVolumes",
        "storagegateway:describeFileSystemAssociations",
        "storagegateway:describeGatewayInformation",
        "storagegateway:describeMaintenanceStartTime",
        "storagegateway:describeNFSFileShares",
        "storagegateway:describeSMBFileShares",
        "storagegateway:describeSMBSettings",
        "storagegateway:describeSnapshotSchedule",
        "storagegateway:describeStorediSCSIVolumes",
        "storagegateway:describeTapeArchives",
        "storagegateway:describeTapeRecoveryPoints",
        "storagegateway:describeTapes",
        "storagegateway:describeUploadBuffer",
        "storagegateway:describeVTLDevices",
        "storagegateway:describeWorkingStorage",
        "storagegateway:listAutomaticTapeCreationPolicies",
        "storagegateway:listFileShares",
        "storagegateway:listFileSystemAssociations",
        "storagegateway:listGateways",
        "storagegateway:listLocalDisks",
        "storagegateway:listTagsForResource",
        "storagegateway:listTapes",
        "storagegateway:listVolumeInitiators",
        "storagegateway:listVolumeRecoveryPoints",
        "storagegateway:listVolumes",
        "swf:countClosedWorkflowExecutions",
        "swf:countOpenWorkflowExecutions",
        "swf:countPendingActivityTasks",
        "swf:countPendingDecisionTasks",
        "swf:describeActivityType",
        "swf:describeDomain",
        "swf:describeWorkflowExecution",
        "swf:describeWorkflowType",
        "swf:getWorkflowExecutionHistory",
        "swf:listActivityTypes",
        "swf:listClosedWorkflowExecutions",
        "swf:listDomains",
        "swf:listOpenWorkflowExecutions",
        "swf:listWorkflowTypes",
        "synthetics:describeCanaries",
        "synthetics:describeCanariesLastRun",
```

```
        "synthetics:describeRuntimeVersions",
        "synthetics:getCanary",
        "synthetics:getCanaryRuns",
        "synthetics:getGroup",
        "synthetics:listAssociatedGroups",
        "synthetics:listGroupResources",
        "synthetics:listGroups",
        "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"
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSSystemsManagerAccountDiscoveryServicePolicy

Deskripsi: Memberi izin kepada AWS Systems Manager (SSM) untuk menemukan Akun AWS informasi.

`AWSSystemsManagerAccountDiscoveryServicePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 24 Oktober 2019, 17:21 UTC
- Waktu yang telah diedit: 17 Oktober 2022, 20.25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerAccountDiscoveryServicePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListRoots",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:ListDelegatedServicesForAccount",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSSystemsManagerChangeManagementServicePolicy

Deskripsi: Menyediakan akses ke AWS sumber daya yang dikelola atau digunakan oleh kerangka kerja manajemen perubahan AWS Systems Manager.

`AWSSystemsManagerChangeManagementServicePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 07 Desember 2020, 22:21 UTC
- Waktu yang telah diedit: 07 Desember 2020, 22:21 UTC

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

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM

- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSSystemsManagerEnableConfigRecordingExecutionPolicy

Deskripsi: Menyediakan izin untuk AWS Systems Manager Quick Setup untuk mengaktifkan dan mengonfigurasi perekaman konfigurasi AWS Config.

`AWSSystemsManagerEnableConfigRecordingExecutionPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSSystemsManagerEnableConfigRecordingExecutionPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 26 Juni 2024, 09:40 UTC
- Waktu telah diedit: 26 Juni 2024, 09:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerEnableConfigRecordingExecutionPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSSystemsManagerEnableExplorerExecutionPolicy

Deskripsi: Kebijakan ini memberikan izin administratif untuk mengaktifkan Explorer, kemampuan Systems Manager AWS . Ini termasuk izin untuk memperbarui setelan layanan Systems Manager terkait, dan untuk membuat peran terkait layanan untuk Systems Manager.

`AWSSystemsManagerEnableExplorerExecutionPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSSystemsManagerEnableExplorerExecutionPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 26 Juni 2024, 09:42 UTC
- Waktu telah diedit: 26 Juni 2024, 09:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerEnableExplorerExecutionPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSSystemsManagerForSAPFullAccess

Deskripsi: Menyediakan akses penuh ke AWS Systems Manager untuk layanan SAP

`AWSSystemsManagerForSAPFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSSystemsManagerForSAPFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 17 November 2022, 02:11 UTC
- Waktu yang telah diedit: 10 Juli 2024, 21:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerForSAPFullAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSSystemsManagerForSAPReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke AWS Systems Manager untuk layanan SAP

`AWSSystemsManagerForSAPReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSSystemsManagerForSAPReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 17 November 2022, 02:11 UTC
- Waktu telah diedit: 17 November 2022, 02:11 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerForSAPReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:get*",
        "ssm-sap:list*"
      ],
      "Resource" : "arn:*:ssm-sap:*:*:*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSSystemsManagerJustInTimeAccessServicePolicy

Deskripsi: Menyediakan akses ke AWS sumber daya yang dikelola atau digunakan oleh AWS Systems Manager hanya dalam kerangka kerja akses waktu.

`AWSSystemsManagerJustInTimeAccessServicePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 21 April 2025, 20:07 UTC
- Waktu yang telah diedit: April 21, 2025, 20:07 UTC

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

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSSystemsManagerJustInTimeAccessTokenPolicy

Deskripsi: Kebijakan terkelola AWSSystems ManagerJustInTimeAccessTokenPolicy memungkinkan Systems Manager menghasilkan token akses yang digunakan untuk akses just-in-time node.

`AWSSystemsManagerJustInTimeAccessTokenPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSSystemsManagerJustInTimeAccessTokenPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 17 April 2025, 21:07 UTC
- Waktu yang telah diedit: 17 April 2025, 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerJustInTimeAccessTokenPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "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" : "TerminateAndResumeSession",
      "Effect" : "Allow",
      "Action" : [
        "ssm:TerminateSession",
        "ssm:ResumeSession"
      ],
      "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"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSSystemsManagerJustInTimeAccessTokenSessionPolicy

Deskripsi: Kebijakan terkelola AWSSystems ManagerJustInTimeAccessTokenSessionPolicy memungkinkan Systems Manager menerapkan izin bawah cakupan ke sesi akses just-in-time node setelah dimulai.

`AWSSystemsManagerJustInTimeAccessTokenSessionPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSSystemsManagerJustInTimeAccessTokenSessionPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 17 April 2025, 20:52 UTC
- Waktu yang telah diedit: 17 April 2025, 20:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerJustInTimeAccessTokenSessionPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy

Deskripsi: Kebijakan ini memungkinkan Systems Manager untuk membagikan kebijakan akses penolakan untuk akses just-in-time node dari akun administrator yang didelegasikan ke akun anggota, dan mereplikasi kebijakan tersebut ke beberapa Wilayah.

`AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 21 April 2025, 20:52 UTC
- Waktu yang telah diedit: 23 April 2025, 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSSystemsManagerNotificationsServicePolicy

Deskripsi: Izin diperlukan untuk mengumpulkan informasi tentang pengguna untuk pemberitahuan Just-In-Time-Node -Access.

`AWSSystemsManagerNotificationsServicePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 17 April 2025, 20:52 UTC
- Waktu yang telah diedit: 17 April 2025, 20:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerNotificationsServicePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSSystemsManagerOpsDataSyncServiceRolePolicy

Deskripsi: Peran IAM untuk SSM Explorer untuk mengelola operasi terkait OpsData

`AWSSystemsManagerOpsDataSyncServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 26 April 2021 20:42 UTC
- Waktu yang telah diedit: 28 Juni 2023, 22:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerOpsDataSyncServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/ExplorerSecurityHubOpsItem" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateOpsItem"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:opsitem/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/*",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "securityhub:GetFindings",
        "securityhub:BatchUpdateFindings"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Deny",
      "Action" : "securityhub:BatchUpdateFindings",
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "securityhub:ASFFSyntaxPath/Workflow.Status" : "SUPPRESSED"
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : "securityhub:BatchUpdateFindings",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "securityhub:ASFFSyntaxPath/Confidence" : false
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : "securityhub:BatchUpdateFindings",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "securityhub:ASFFSyntaxPath/Criticality" : false
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : "securityhub:BatchUpdateFindings",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "securityhub:ASFFSyntaxPath/Note.Text" : false
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : "securityhub:BatchUpdateFindings",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "securityhub:ASFFSyntaxPath/Note.UpdatedBy" : false
```

```
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : "securityhub:BatchUpdateFindings",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "securityhub:ASFFSyntaxPath/RelatedFindings" : false
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : "securityhub:BatchUpdateFindings",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "securityhub:ASFFSyntaxPath/Types" : false
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : "securityhub:BatchUpdateFindings",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "securityhub:ASFFSyntaxPath/UserDefinedFields.key" : false
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : "securityhub:BatchUpdateFindings",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "securityhub:ASFFSyntaxPath/UserDefinedFields.value" : false
        }
      }
    },
    {
```

```
      "Effect" : "Deny",
      "Action" : "securityhub:BatchUpdateFindings",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "securityhub:ASFFSyntaxPath/VerificationState" : false
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSThinkboxAssetServerPolicy

Deskripsi: Kebijakan ini memberi Server Aset AWS Portal izin yang diperlukan untuk pengoperasian normal.

`AWSThinkboxAssetServerPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSThinkboxAssetServerPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Mei 2020, 19:18 UTC
- Waktu yang telah diedit: 27 Mei 2020, 19:18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxAssetServerPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/thinkbox*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-portal-cache*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSThinkboxAWSPortalAdminPolicy

Deskripsi: Kebijakan ini memberikan perangkat lunak Tenggat Waktu AWS Thinkbox akses penuh ke beberapa AWS layanan seperti yang diperlukan untuk administrasi Portal. AWS Ini termasuk akses untuk membuat tag arbitrer pada beberapa jenis EC2 sumber daya.

`AWSThinkboxAWSPortalAdminPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSThinkboxAWSPortalAdminPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Mei 2020, 19:41 UTC
- Waktu telah diedit: 12 November 2024, 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxAWSPortalAdminPolicy`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSThinkboxAWSPortal1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachInternetGateway",
        "ec2:AssociateAddress",
        "ec2:AssociateRouteTable",
```

```
        "ec2:AllocateAddress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateFleet",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateInternetGateway",
        "ec2:CreateNatGateway",
        "ec2:CreatePlacementGroup",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateVpc",
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeAddresses",
        "ec2:DescribeFleets",
        "ec2:DescribeFleetHistory",
        "ec2:DescribeFleetInstances",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeRouteTables",
        "ec2:DescribeNatGateways",
        "ec2:DescribeTags",
        "ec2:DescribeKeyPairs",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeRegions",
        "ec2:DescribeSpotFleetRequestHistory",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSpotFleetInstances",
        "ec2:DescribeSpotFleetRequests",
        "ec2:DescribeSpotPriceHistory",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:GetConsoleOutput",
        "ec2:ImportKeyPair",
        "ec2:ReleaseAddress",
        "ec2:RequestSpotFleet",
        "ec2:CancelSpotFleetRequests",
        "ec2:DisassociateAddress",
        "ec2:DeleteFleets",
```

```
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteVpc",
        "ec2:DeletePlacementGroup",
        "ec2:DeleteVpcEndpoints",
        "ec2:DeleteInternetGateway",
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
        "ec2:DisassociateRouteTable",
        "ec2:DeleteSubnet",
        "ec2:DeleteNatGateway",
        "ec2:DetachInternetGateway",
        "ec2:ModifyInstanceAttribute",
        "ec2:ModifyFleet",
        "ec2:ModifySpotFleetRequest",
        "ec2:ModifyVpcAttribute"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSThinkboxAWSPortal2",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:placement-group/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*::image/*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal3",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "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*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSThinkboxAWSPortalGatewayPolicy

Deskripsi: Kebijakan ini memberi mesin AWS Portal Gateway izin yang diperlukan untuk pengoperasian normal.

`AWSThinkboxAWSPortalGatewayPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSThinkboxAWSPortalGatewayPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Mei 2020, 19:05 UTC
- Waktu yang telah diedit: 30 Juni 2020, 16:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxAWSPortalGatewayPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-portal-cache*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "dynamodb:Scan",
      "Resource" : [
        "arn:aws:dynamodb:*:*:table/DeadlineFleetHealth*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::stack*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::stack*/gateway_certs/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : [
```

```
        "arn:aws:secretsmanager:*:*:secret:rcs-tls-pw-stack*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSThinkboxAWSPortalWorkerPolicy

Deskripsi: Kebijakan ini memberi Batas Waktu Pekerja di AWS Portal izin yang diperlukan untuk operasi normal.

`AWSThinkboxAWSPortalWorkerPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSThinkboxAWSPortalWorkerPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Mei 2020, 19:15 UTC
- Waktu yang telah diedit: 07 Desember 2020, 23:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxAWSPortalWorkerPolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeTags"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/DeadlineRole" : "DeadlineRenderNode"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-portal-cache*"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::stack*/gateway_certs/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/thinkbox*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:SendMessage",
        "sqs:GetQueueUrl"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:DeadlineAWS*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSThinkboxDeadlineResourceTrackerAccessPolicy

Deskripsi: Memberikan izin yang diperlukan untuk pengoperasian AWS Thinkbox's Deadline Resource Tracker. Ini termasuk akses penuh ke beberapa EC2 tindakan, termasuk DeleteFleets dan CancelSpotFleetRequests.

`AWSThinkboxDeadlineResourceTrackerAccessPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSThinkboxDeadlineResourceTrackerAccessPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Mei 2020, 19:25 UTC
- Waktu yang telah diedit: 27 Mei 2020, 19:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxDeadlineResourceTrackerAccessPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListStreams"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:BatchWriteItem",
        "dynamodb:DeleteItem",
        "dynamodb:DescribeStream",
        "dynamodb:DescribeTable",
        "dynamodb:GetItem",
        "dynamodb:GetRecords",
        "dynamodb:GetShardIterator",
        "dynamodb:PutItem",
        "dynamodb:Scan",
        "dynamodb:UpdateItem",
        "dynamodb:UpdateTable"
      ],
      "Resource" : [
        "arn:aws:dynamodb:*:*:table/DeadlineEC2ComputeNodeHealth*",
        "arn:aws:dynamodb:*:*:table/DeadlineEC2ComputeNodeInfo*",
        "arn:aws:dynamodb:*:*:table/DeadlineFleetHealth*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CancelSpotFleetRequests",
        "ec2:DeleteFleets",
        "ec2:DescribeFleetInstances",
        "ec2:DescribeFleets",
        "ec2:DescribeInstances",
```

```
        "ec2:DescribeSpotFleetInstances",
        "ec2:DescribeSpotFleetRequests"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RebootInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/DeadlineTrackedAWSResource" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:PutEvents"
      ],
      "Resource" : [
        "arn:aws:events:*:*:event-bus/default"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:DeadlineResourceTracker*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
```

```
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/lambda/DeadlineResourceTracker*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:DeleteMessage",
        "sqs:GetQueueAttributes",
        "sqs:ReceiveMessage"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:DeadlineAWSComputeNodeStateMessageQueue*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSThinkboxDeadlineResourceTrackerAdminPolicy

Deskripsi: Memberikan izin yang diperlukan untuk membuat, menghancurkan, dan mengelola Pelacak Sumber Daya Tenggat AWS Thinkbox.

`AWSThinkboxDeadlineResourceTrackerAdminPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSThinkboxDeadlineResourceTrackerAdminPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Mei 2020, 19:29 UTC
- Waktu telah diedit: 12 November 2024, 19:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxDeadlineResourceTrackerAdminPolicy`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSThinkboxDeadlineSpotEventPluginAdminPolicy

Deskripsi: Memberikan izin yang diperlukan untuk Plugin Acara Spot Tenggat Waktu AWS Thinkbox. Ini termasuk izin untuk meminta, memodifikasi, dan membatalkan armada spot, serta PassRole izin terbatas.

`AWSThinkboxDeadlineSpotEventPluginAdminPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSThinkboxDeadlineSpotEventPluginAdminPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Mei 2020, 19:38 UTC
- Waktu yang telah diedit: 27 Mei 2020, 19:38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxDeadlineSpotEventPluginAdminPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CancelSpotFleetRequests",
        "ec2:DescribeSpotFleetInstances",
        "ec2:DescribeSpotFleetRequests",
        "ec2:ModifySpotFleetRequest",
        "ec2:RequestSpotFleet"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "RunInstances"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:ec2spot:fleet-request-id" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "spot.amazonaws.com",
            "spotfleet.amazonaws.com"
```

```
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-ec2-spot-fleet-tagging-role",
        "arn:aws:iam::*:role/DeadlineSpot*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetUser"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-ec2-spot-fleet-tagging-role",
        "arn:aws:iam::*:role/DeadlineSpot*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
```

```
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSThinkboxDeadlineSpotEventPluginWorkerPolicy

Deskripsi: Berikan izin yang diperlukan untuk EC2 instance yang menjalankan perangkat lunak AWS Thinkbox Deadline Spot Event Plugin Worker.

`AWSThinkboxDeadlineSpotEventPluginWorkerPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSThinkboxDeadlineSpotEventPluginWorkerPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Mei 2020, 19:35 UTC
- Waktu yang telah diedit: 07 Desember 2020, 23:31 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxDeadlineSpotEventPluginWorkerPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeTags"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/DeadlineTrackedAWSResource" : "SpotEventPlugin"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "ec2:ResourceTag/DeadlineResourceTracker" : "SpotEventPlugin"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:GetQueueUrl",
        "sqs:SendMessage"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:DeadlineAWSComputeNodeState*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSTransferConsoleFullAccess

Deskripsi: Menyediakan akses penuh ke AWS Transfer melalui AWS Management Console

`AWSTransferConsoleFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSTransferConsoleFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 14 Desember 2020 19:33 UTC

- Waktu yang telah diedit: 14 Desember 2020, 19:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransferConsoleFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "transfer.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:ListCertificates",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "health:DescribeEventAggregates",
        "iam:GetPolicyVersion",
        "iam:ListPolicies",
        "iam:ListRoles",
```

```
        "route53:ListHostedZones",
        "s3:ListAllMyBuckets",
        "transfer:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSTransferFullAccess

Deskripsi: Menyediakan akses penuh ke Layanan AWS Transfer.

`AWSTransferFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSTransferFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 14 Desember 2020 19:37 UTC
- Waktu yang telah diedit: 14 Desember 2020, 19:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransferFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "transfer:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "transfer.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAddresses"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSTransferLoggingAccess

Deskripsi: Memungkinkan AWS Transfer akses penuh untuk membuat aliran log dan grup dan menempatkan peristiwa log ke akun Anda

`AWSTransferLoggingAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSTransferLoggingAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 14 Januari 2019, 15:32 UTC
- Waktu yang telah diedit: 14 Januari 2019, 15:32 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSTransferLoggingAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
        "logs:DescribeLogStreams",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSTransferReadOnlyAccess

Deskripsi: Menyediakan akses readonly ke layanan AWS Transfer.

`AWSTransferReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSTransferReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Agustus 2020, 17:54 UTC
- Waktu yang telah diedit: 27 Agustus 2020, 17:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransferReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "transfer:DescribeUser",
        "transfer:DescribeServer",
        "transfer:ListUsers",
        "transfer:ListServers",
        "transfer:TestIdentityProvider",
        "transfer:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSTrustedAdvisorPriorityFullAccess

Deskripsi: Menyediakan akses penuh ke Prioritas AWS Trusted Advisor. Kebijakan ini juga memungkinkan pengguna untuk menambahkan Trusted Advisor sebagai layanan tepercaya dengan AWS Organizations dan menentukan akun administrator yang didelegasikan untuk Prioritas Trusted Advisor.

`AWSTrustedAdvisorPriorityFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSTrustedAdvisorPriorityFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 16 Agustus 2022, 16:08 UTC
- Waktu yang telah diedit: 16 Agustus 2022, 16.08 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTrustedAdvisorPriorityFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "trustedadvisor:DescribeAccount*",
        "trustedadvisor:DescribeOrganization",
        "trustedadvisor:DescribeRisk*",
        "trustedadvisor:DownloadRisk",
        "trustedadvisor:UpdateRiskStatus",
        "trustedadvisor:DescribeNotificationConfigurations",
        "trustedadvisor:UpdateNotificationConfigurations",
        "trustedadvisor:DeleteNotificationConfigurationForDelegatedAdmin",
        "trustedadvisor:SetOrganizationAccess"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators",
        "organizations:EnableAWSServiceAccess",
        "organizations:DisableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "reporting.trustedadvisor.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
reporting.trustedadvisor.amazonaws.com/AWSServiceRoleForTrustedAdvisorReporting",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "reporting.trustedadvisor.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource" : "arn:aws:organizations::*:*",
      "Condition" : {
```

```
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "reporting.trustedadvisor.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin dengan hak istimewa paling sedikit

AWSTrustedAdvisorPriorityReadOnlyAccess

Deskripsi: Menyediakan akses hanya-baca ke Prioritas Trusted AWS Advisor. Ini termasuk izin untuk melihat akun administrator yang didelegasikan.

`AWSTrustedAdvisorPriorityReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSTrustedAdvisorPriorityReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 16 Agustus 2022, 16:35 UTC
- Waktu yang telah diedit: 16 Agustus 2022, 16.35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTrustedAdvisorPriorityReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "trustedadvisor:DescribeAccount*",
        "trustedadvisor:DescribeOrganization",
        "trustedadvisor:DescribeRisk*",
        "trustedadvisor:DownloadRisk",
        "trustedadvisor:DescribeNotificationConfigurations"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "reporting.trustedadvisor.amazonaws.com"
          ]
```

```
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSTrustedAdvisorReportingServiceRolePolicy

Deskripsi: Kebijakan Layanan untuk Pelaporan Multi-Akun Trusted Advisor

`AWSTrustedAdvisorReportingServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 19 November 2019, 17:41 UTC
- Waktu telah diedit: 28 Februari 2023, 23:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSTrustedAdvisorReportingServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSTrustedAdvisorServiceRolePolicy

Deskripsi: Akses ke Layanan AWS Trusted Advisor untuk membantu mengurangi biaya, meningkatkan kinerja, dan meningkatkan keamanan lingkungan Anda AWS .

`AWSTrustedAdvisorServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 22 Februari 2018, 21:24 UTC
- Waktu yang telah diedit: 30 Oktober 2024, 16:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSTrustedAdvisorServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v14 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSUserNotificationsServiceLinkedRolePolicy

Deskripsi: Memungkinkan Pemberitahuan AWS Pengguna untuk memanggil AWS layanan atas nama Anda.

`AWSUserNotificationsServiceLinkedRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan

- Waktu pembuatan: 19 April 2023, 13:28 UTC
- Waktu telah diedit: 14 Januari 2025, 23:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSUserNotificationsServiceLinkedRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:PutRule",
        "events:PutTargets",
        "events:DeleteRule",
        "events:ListTargetsByRule",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/AWSUserNotificationsManagedRule-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Notifications"
        }
      },
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "AllowOrgsActions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListChildren",
        "organizations:ListParents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSVendorInsightsAssessorFullAccess

Deskripsi: Menyediakan akses penuh untuk melihat sumber daya Vendor Insights yang berjudul dan mengelola langganan Vendor Insights

`AWSVendorInsightsAssessorFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSVendorInsightsAssessorFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 26 Juli 2022, 15:05 UTC
- Waktu yang telah diedit: 01 Desember 2022 00:51 UTC

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

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "vendor-insights:GetProfileAccessTerms",
        "vendor-insights:ListEntitledSecurityProfiles",
        "vendor-insights:GetEntitledSecurityProfileSnapshot",
        "vendor-insights:ListEntitledSecurityProfileSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:CreateAgreementRequest",
        "aws-marketplace:GetAgreementRequest",
        "aws-marketplace:AcceptAgreementRequest",
        "aws-marketplace:CancelAgreementRequest",
        "aws-marketplace:ListAgreementRequests",
        "aws-marketplace:SearchAgreements",
        "aws-marketplace:CancelAgreement"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws-marketplace:AgreementType" : "VendorInsightsAgreement"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports"
      ],
      "Resource" : "arn:aws:artifact:*::report/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSVendorInsightsAssessorReadOnly

Deskripsi: Menyediakan akses hanya-baca untuk melihat sumber daya Vendor Insights yang berjudul

`AWSVendorInsightsAssessorReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSVendorInsightsAssessorReadOnly` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 26 Juli 2022, 15:05 UTC
- Waktu telah diedit: 01 Desember 2022, 00:55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSVendorInsightsAssessorReadOnly`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "vendor-insights:ListEntitledSecurityProfiles",
        "vendor-insights:GetEntitledSecurityProfileSnapshot",
        "vendor-insights:ListEntitledSecurityProfileSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports"
      ],
      "Resource" : "arn:aws:artifact:*::report/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSVendorInsightsVendorFullAccess

Deskripsi: Menyediakan akses penuh untuk membuat dan mengelola sumber daya Vendor Insights

`AWSVendorInsightsVendorFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSVendorInsightsVendorFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 26 Juli 2022, 15:05 UTC
- Waktu telah diedit: 19 Oktober 2023, 01:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSVendorInsightsVendorFullAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "aws-marketplace:DescribeEntity",
      "Resource" : "arn:aws:aws-marketplace:*:*:*/SaaSProduct/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "aws-marketplace:ListEntities",
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "vendor-insights:CreateDataSource",
        "vendor-insights:UpdateDataSource",
        "vendor-insights:DeleteDataSource",
        "vendor-insights:GetDataSource",
        "vendor-insights:ListDataSources",
        "vendor-insights:CreateSecurityProfile",
        "vendor-insights:ListSecurityProfiles",
        "vendor-insights:GetSecurityProfile",
        "vendor-insights:AssociateDataSource",
        "vendor-insights:DisassociateDataSource",
        "vendor-insights:UpdateSecurityProfile",
        "vendor-insights:ActivateSecurityProfile",
        "vendor-insights:DeactivateSecurityProfile",
        "vendor-insights:UpdateSecurityProfileSnapshotCreationConfiguration",
        "vendor-insights:UpdateSecurityProfileSnapshotReleaseConfiguration",
        "vendor-insights:ListSecurityProfileSnapshots",
        "vendor-insights:GetSecurityProfileSnapshot",
        "vendor-insights:TagResource",
        "vendor-insights:UntagResource",
        "vendor-insights:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:AcceptAgreementApprovalRequest",
        "aws-marketplace:RejectAgreementApprovalRequest",
        "aws-marketplace:GetAgreementApprovalRequest",
        "aws-marketplace:ListAgreementApprovalRequests",
        "aws-marketplace:CancelAgreement",
        "aws-marketplace:SearchAgreements"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws-marketplace:AgreementType" : "VendorInsightsAgreement"
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports"
      ],
      "Resource" : "arn:aws:artifact:*::report/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSVendorInsightsVendorReadOnly

Deskripsi: Menyediakan akses hanya-baca untuk melihat sumber daya Vendor Insights

`AWSVendorInsightsVendorReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSVendorInsightsVendorReadOnly` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 26 Juli 2022, 15:05 UTC
- Waktu yang telah diedit: 01 Desember 2022 00:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSVendorInsightsVendorReadOnly`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "aws-marketplace:DescribeEntity",
      "Resource" : "arn:aws:aws-marketplace:*:*:*/SaaSProduct/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "aws-marketplace:ListEntities",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "vendor-insights:GetDataSource",
        "vendor-insights:ListDataSources",
        "vendor-insights:ListSecurityProfiles",
        "vendor-insights:GetSecurityProfile",
        "vendor-insights:GetSecurityProfileSnapshot",
        "vendor-insights:ListSecurityProfileSnapshots",
        "vendor-insights:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports"
```

```
      ],
      "Resource" : "arn:aws:artifact:*::report/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSVpcLatticeServiceRolePolicy

Deskripsi: Memungkinkan VPC Lattice mengakses AWS sumber daya atas nama Anda.

`AWSVpcLatticeServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 30 November 2022, 20:47 UTC
- Waktu yang telah diedit: 01 Desember 2024, 14:06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVpcLatticeServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSVPCS2SVpnServiceRolePolicy

Deskripsi: Izinkan Site-to-Site VPN membuat dan mengelola sumber daya yang terkait dengan Koneksi VPN Anda.

`AWSVPCS2SVpnServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 06 Agustus 2019 14:13 UTC
- Waktu yang telah diedit: 15 Mei 2025, 16:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVPCS2SVpnServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSVPCTransitGatewayServiceRolePolicy

Deskripsi: Izinkan Gateway Transit VPC membuat dan mengelola sumber daya yang diperlukan untuk Lampiran VPC Gateway Transit Anda.

`AWSVPCTransitGatewayServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 26 November 2018, 16:21 UTC
- Waktu yang telah diedit: 15 April 2021, 16.31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVPCTransitGatewayServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSVPCVerifiedAccessServiceRolePolicy

Deskripsi: Kebijakan untuk mengaktifkan layanan Akses AWS Terverifikasi untuk menyediakan titik akhir atas nama Anda

`AWSVPCVerifiedAccessServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 29 November 2022, 03:35 UTC
- Waktu telah diedit: 17 November 2023, 21:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVPCVerifiedAccessServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VerifiedAccessRoleModifyTaggedNetworkInterfaceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/VerifiedAccessManaged" : "true"
        }
      }
    },
    {
      "Sid" : "VerifiedAccessRoleModifyNetworkInterfaceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*"
    },
    {
      "Sid" : "VerifiedAccessRoleNetworkInterfaceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
```

```
      "Sid" : "VerifiedAccessRoleTaggedNetworkInterfaceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/VerifiedAccessManaged" : "true"
        }
      }
    },
    {
      "Sid" : "VerifiedAccessRoleTaggingActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSWAFConsoleFullAccess

Deskripsi: Menyediakan akses penuh ke AWS WAF melalui. AWS Management Console Perhatikan bahwa kebijakan ini juga memberikan izin untuk mencantumkan dan memperbarui CloudFront distribusi Amazon, izin untuk melihat penyeimbang beban di Elastic Load AWS Balancing, izin untuk melihat REST dan tahapan Amazon API Gateway, izin untuk membuat daftar dan melihat metrik Amazon, dan izin untuk melihat wilayah CloudWatch yang diaktifkan dalam akun. APIs

`AWSWAFConsoleFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSWAFConsoleFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 April 2020, 18:38 UTC
- Waktu telah diedit: 05 Mei 2025, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWAFConsoleFullAccess`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "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: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" : "*"
    },
    {
      "Sid" : "AllowActionsForAppSync",
      "Effect" : "Allow",
      "Action" : [
        "appsync:SetWebACL"
      ],
      "Resource" : "arn:aws:appsync:*:*:apis/*"
    },
    {
      "Sid" : "AllowListActionsForAppSync",
      "Effect" : "Allow",
      "Action" : [
        "appsync:ListGraphqlApis"
      ],
      "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" : "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"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSWAFConsoleReadOnlyAccess

Deskripsi: Menyediakan akses hanya-baca ke AWS WAF melalui. AWS Management Console Perhatikan bahwa kebijakan ini juga memberikan izin untuk mencantumkan CloudFront distribusi Amazon, izin untuk melihat penyeimbang beban di Elastic Load AWS Balancing, izin untuk melihat REST dan tahapan Amazon API Gateway, izin untuk membuat daftar dan melihat metrik Amazon, dan izin untuk melihat wilayah CloudWatch yang diaktifkan dalam akun. APIs

`AWSWAFConsoleReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSWAFConsoleReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 April 2020, 18:43 UTC
- Waktu telah diedit: 05 Mei 2025, 21:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWAFConsoleReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "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"
      ],
      "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" : "*"
    },
    {
      "Sid" : "AllowListActionsForAppSync",
      "Effect" : "Allow",
      "Action" : [
        "appsync:ListGraphqlApis"
      ],
      "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" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSWAFFullAccess

Deskripsi: Menyediakan akses penuh ke tindakan AWS WAF.

`AWSWAFFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSWAFFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Oktober 2015, 20:44 UTC

- Waktu yang telah diedit: 05 Mei 2025, 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWAFFullAccess`

Versi kebijakan

Versi kebijakan: v12 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSWAFReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke tindakan AWS WAF.

`AWSWAFReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSWAFReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Oktober 2015, 20:43 UTC
- Waktu yang telah diedit: 05 Mei 2025, 21:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWAFReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSWellArchitectedDiscoveryServiceRolePolicy

Deskripsi: Memungkinkan WellArchitected untuk mengakses AWS layanan dan sumber daya yang berhubungan dengan WellArchitected sumber daya atas nama pelanggan.

`AWSWellArchitectedDiscoveryServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 26 April 2023, 18:36 UTC
- Waktu telah diedit: 26 April 2023, 18:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSWellArchitectedDiscoveryServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "trustedadvisor:DescribeChecks",
        "trustedadvisor:DescribeCheckItems"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "resource-groups:ListGroupResources",
        "tag:GetResources"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:ListAssociatedResources",
        "servicecatalog:GetApplication",
        "servicecatalog:CreateAttributeGroup"
      ],
      "Resource" : [
```

```
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:AssociateAttributeGroup",
        "servicecatalog:DisassociateAttributeGroup"
      ],
      "Resource" : [
        "arn:*:servicecatalog:*:*:/applications/*",
        "arn:*:servicecatalog:*:*:/attribute-groups/AWS_WellArchitected-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:UpdateAttributeGroup",
        "servicecatalog:DeleteAttributeGroup"
      ],
      "Resource" : [
        "arn:*:servicecatalog:*:*:/attribute-groups/AWS_WellArchitected-*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSWellArchitectedOrganizationsServiceRolePolicy

Deskripsi: Memungkinkan Well-Architected untuk mengakses Organizations atas nama Anda.

`AWSWellArchitectedOrganizationsServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 23 Juni 2022, 17:15 UTC
- Waktu yang telah diedit: 25 Juli 2022, 18.03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSWellArchitectedOrganizationsServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:ListRoots"
```

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSWickrFullAccess

Deskripsi: Kebijakan ini memberikan izin administratif penuh ke layanan Wickr, termasuk fungsi administratif Wickr di bawah. AWS Management Console

`AWSWickrFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSWickrFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 November 2022, 20:36 UTC
- Waktu yang telah diedit: 27 November 2022 20.36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWickrFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSXrayCrossAccountSharingConfiguration

Deskripsi: Menyediakan kemampuan untuk mengelola tautan Observability Access Manager dan membangun berbagi jejak X-Ray

`AWSXrayCrossAccountSharingConfiguration`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSXrayCrossAccountSharingConfiguration` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 November 2022, 13:46 UTC
- Waktu yang telah diedit: 27 November 2022, 13.46 UTC

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

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:Link",
        "oam:ListLinks"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:DeleteLink",
        "oam:GetLink",
        "oam:TagResource"
      ],
      "Resource" : "arn:aws:oam:*:*:link/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:CreateLink",
        "oam:UpdateLink"
      ],
      "Resource" : [
        "arn:aws:oam:*:*:link/*",
        "arn:aws:oam:*:*:sink/*"
      ]
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSXRayDaemonWriteAccess

Deskripsi: Izinkan Daemon AWS X-Ray menyampaikan data segmen jejak mentah ke API layanan dan mengambil data pengambilan sampel (aturan, target, dll.) untuk digunakan oleh X-Ray SDK.

`AWSXRayDaemonWriteAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSXRayDaemonWriteAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 Agustus 2018, 23:00 UTC
- Waktu telah diedit: 13 Februari 2024, 21:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXRayDaemonWriteAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSXRayDaemonWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSXrayFullAccess

Deskripsi: Kebijakan terkelola akses penuh AWS X-Ray

`AWSXrayFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSXrayFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Desember 2016, 18:30 UTC
- Waktu yang telah diedit: 11 April 2024, 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXrayFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSXrayReadOnlyAccess

Deskripsi: AWS X-Ray hanya membaca kebijakan terkelola

`AWSXrayReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSXrayReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Desember 2016, 18:27 UTC
- Waktu yang telah diedit: 14 Februari 2024, 00:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXrayReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSXrayReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
```

```
        "xray:GetSamplingStatisticSummaries",
        "xray:BatchGetTraces",
        "xray:BatchGetTraceSummaryById",
        "xray:GetDistinctTraceGraphs",
        "xray:GetServiceGraph",
        "xray:GetTraceGraph",
        "xray:GetTraceSummaries",
        "xray:GetGroups",
        "xray:GetGroup",
        "xray:ListTagsForResource",
        "xray:ListResourcePolicies",
        "xray:GetTimeSeriesServiceStatistics",
        "xray:GetInsightSummaries",
        "xray:GetInsight",
        "xray:GetInsightEvents",
        "xray:GetInsightImpactGraph"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSXrayWriteOnlyAccess

Deskripsi: AWS X-Ray menulis hanya kebijakan terkelola

`AWSXrayWriteOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSXrayWriteOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Desember 2016, 18:19 UTC
- Waktu telah diedit: 28 Agustus 2018, 23:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXrayWriteOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSZonalAutoshiftPracticeRunSLRPolicy

Deskripsi: Menyediakan akses administratif untuk menjalankan praktik pergeseran zona ARC, dan akses ke status CloudWatch alarm untuk memantau praktik berjalan.

`AWSZonalAutoshiftPracticeRunSLRPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 29 November 2023, 17:34 UTC
- Waktu yang telah diedit: 30 Juni 2025, 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSZonalAutoshiftPracticeRunSLRPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSZoneGroupAccessManagementServiceRolePolicy

Deskripsi: Menyediakan akses hanya-baca ke yang APIs diperlukan untuk mendukung manajemen akses kelompok-zona untuk organisasi.

`AWSZoneGroupAccessManagementServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 01 Juli 2025, 19:07 UTC
- Waktu yang telah diedit: 01 Juli 2025, 19:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSZoneGroupAccessManagementServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

BatchServiceRolePolicy

Deskripsi: Menyediakan akses ke layanan AWS Batch untuk mengelola sumber daya yang diperlukan, termasuk sumber daya Amazon EC2 dan Amazon ECS.

`BatchServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 10 Maret 2021, 06:55 UTC
- Waktu telah diedit: 05 Desember 2023, 22:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/BatchServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSBatchPolicyStatement1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeImages",
        "ec2:DescribeImageAttribute",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSpotFleetInstances",
        "ec2:DescribeSpotFleetRequests",
        "ec2:DescribeSpotPriceHistory",
        "ec2:DescribeSpotFleetRequestHistory",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:RequestSpotFleet",
        "autoscaling:DescribeAccountLimits",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeLaunchConfigurations",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeScalingActivities",
        "eks:DescribeCluster",
        "ecs:DescribeClusters",
        "ecs:DescribeContainerInstances",
        "ecs:DescribeTaskDefinition",
```

```
        "ecs:DescribeTasks",
        "ecs:ListClusters",
        "ecs:ListContainerInstances",
        "ecs:ListTaskDefinitionFamilies",
        "ecs:ListTaskDefinitions",
        "ecs:ListTasks",
        "ecs:DeregisterTaskDefinition",
        "ecs:TagResource",
        "ecs:ListAccountSettings",
        "logs:DescribeLogGroups",
        "iam:GetInstanceProfile",
        "iam:GetRole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSBatchPolicyStatement2",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/batch/job*"
    },
    {
      "Sid" : "AWSBatchPolicyStatement3",
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/batch/job*:log-stream:*"
    },
    {
      "Sid" : "AWSBatchPolicyStatement4",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:CreateOrUpdateTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSBatchServiceTag" : "false"
        }
      }
```

```
    },
    {
      "Sid" : "AWSBatchPolicyStatement5",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn",
            "ecs-tasks.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AWSBatchPolicyStatement6",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "spot.amazonaws.com",
            "spotfleet.amazonaws.com",
            "autoscaling.amazonaws.com",
            "ecs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AWSBatchPolicyStatement7",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSBatchServiceTag" : "false"
```

```
        }
      }
    },
    {
      "Sid" : "AWSBatchPolicyStatement8",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances",
        "ec2:CancelSpotFleetRequests",
        "ec2:ModifySpotFleetRequest",
        "ec2:DeleteLaunchTemplate"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSBatchServiceTag" : "false"
        }
      }
    },
    {
      "Sid" : "AWSBatchPolicyStatement9",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:CreateLaunchConfiguration",
        "autoscaling:DeleteLaunchConfiguration"
      ],
      "Resource" :
 "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/AWSBatch*"
    },
    {
      "Sid" : "AWSBatchPolicyStatement10",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:CreateAutoScalingGroup",
        "autoscaling:UpdateAutoScalingGroup",
        "autoscaling:SetDesiredCapacity",
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:SuspendProcesses",
        "autoscaling:PutNotificationConfiguration",
        "autoscaling:TerminateInstanceInAutoScalingGroup"
      ],
      "Resource" : "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/
AWSBatch*"
    },
```

```
    {
      "Sid" : "AWSBatchPolicyStatement11",
      "Effect" : "Allow",
      "Action" : [
        "ecs:DeleteCluster",
        "ecs:DeregisterContainerInstance",
        "ecs:RunTask",
        "ecs:StartTask",
        "ecs:StopTask"
      ],
      "Resource" : "arn:aws:ecs:*:*:cluster/AWSBatch*"
    },
    {
      "Sid" : "AWSBatchPolicyStatement12",
      "Effect" : "Allow",
      "Action" : [
        "ecs:RunTask",
        "ecs:StartTask",
        "ecs:StopTask"
      ],
      "Resource" : "arn:aws:ecs:*:*:task-definition/*"
    },
    {
      "Sid" : "AWSBatchPolicyStatement13",
      "Effect" : "Allow",
      "Action" : [
        "ecs:StopTask"
      ],
      "Resource" : "arn:aws:ecs:*:*:task/*/*"
    },
    {
      "Sid" : "AWSBatchPolicyStatement14",
      "Effect" : "Allow",
      "Action" : [
        "ecs:CreateCluster",
        "ecs:RegisterTaskDefinition"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSBatchServiceTag" : "false"
        }
      }
    },
```

```
    {
      "Sid" : "AWSBatchPolicyStatement15",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:placement-group/*",
        "arn:aws:ec2:*:*:capacity-reservation/*",
        "arn:aws:ec2:*:*:elastic-gpu/*",
        "arn:aws:elastic-inference:*:*:elastic-inference-accelerator/*",
        "arn:aws:resource-groups:*:*:group/*"
      ]
    },
    {
      "Sid" : "AWSBatchPolicyStatement16",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSBatchServiceTag" : "false"
        }
      }
    },
    {
      "Sid" : "AWSBatchPolicyStatement17",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances",
```

```
            "CreateLaunchTemplate",
            "RequestSpotFleet"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

Billing

Deskripsi: Memberikan izin untuk penagihan dan manajemen biaya. Ini termasuk melihat penggunaan akun dan melihat serta memodifikasi anggaran dan metode pembayaran.

`Billing`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `Billing` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan fungsi Job
- Waktu pembuatan: 10 November 2016, 17:33 UTC
- Waktu yang telah diedit: 12 Maret 2025, 18:07 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/Billing`

Versi kebijakan

Versi kebijakan: v15 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "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:ListInvoiceSummaries",
        "invoicing:ListInvoiceUnits",
        "invoicing:ListTagsForResource",
        "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" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

CertificateManagerServiceRolePolicy

Deskripsi: Kebijakan Peran Layanan Amazon Certificate Manager

`CertificateManagerServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 25 Juni 2020, 17:56 UTC
- Waktu yang telah diedit: 25 Juni 2020, 17:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CertificateManagerServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

ClientVPNServiceConnectionsRolePolicy

Deskripsi: Kebijakan untuk mengaktifkan AWS Client VPN mengelola koneksi endpoint Client VPN Anda.

`ClientVPNServiceConnectionsRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 12 Agustus 2020, 19:48 UTC
- Waktu yang telah diedit: 12 Agustus 2020, 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ClientVPNServiceConnectionsRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:AWSClientVPN-*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

ClientVPNServiceRolePolicy

Deskripsi: Kebijakan untuk mengaktifkan AWS Client VPN mengelola titik akhir Client VPN Anda.

`ClientVPNServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 10 Desember 2018, 21:20 UTC
- Waktu yang telah diedit: 12 Agustus 2020, 19:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ClientVPNServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeInternetGateways",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeAccountAttributes",
        "ds:AuthorizeApplication",
        "ds:DescribeDirectories",
        "ds:GetDirectoryLimits",
        "ds:UnauthorizeApplication",
        "logs:DescribeLogStreams",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogGroups",
        "acm:GetCertificate",
        "acm:DescribeCertificate",
        "iam:GetSAMLProvider",
        "lambda:GetFunctionConfiguration"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM

- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

CloudFormationStackSetsOrgAdminServiceRolePolicy

Deskripsi: Peran Layanan untuk CloudFormation StackSets (Akun Master Organisasi)

`CloudFormationStackSetsOrgAdminServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 10 Desember 2019 00:20 UTC
- Waktu diedit: 10 Desember 2019, 00:20 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudFormationStackSetsOrgAdminServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      "Effect" : "Allow",
      "Action" : [
        "organizations:List*",
        "organizations:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAssumeRoleInMemberAccounts",
      "Effect" : "Allow",
      "Action" : "sts:AssumeRole",
      "Resource" : "arn:aws:iam::*:role/stacksets-exec-*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

CloudFormationStackSetsOrgMemberServiceRolePolicy

Deskripsi: Peran Layanan untuk CloudFormation StackSets (Akun Anggota Organisasi)

`CloudFormationStackSetsOrgMemberServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 09 Desember 2019, 23:52 UTC
- Waktu yang telah diedit: 09 Desember 2019, 23:52 UTC

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

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:GetRole"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/stacksets-exec-*"
      ]
    },
    {
      "Action" : [
        "iam:DetachRolePolicy",
        "iam:AttachRolePolicy"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/stacksets-exec-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PolicyARN" : "arn:aws:iam::aws:policy/AdministratorAccess"
        }
      }
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

CloudFrontFullAccess

Deskripsi: Menyediakan akses penuh ke CloudFront konsol ditambah kemampuan untuk membuat daftar bucket Amazon S3 melalui. AWS Management Console

`CloudFrontFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudFrontFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:39 UTC
- Waktu yang telah diedit: 28 April 2025, 16:52 UTC
- ARN: `arn:aws:iam::aws:policy/CloudFrontFullAccess`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
  "Statement" : [
    {
      "Sid" : "cfflistbuckets",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "cffullaccess",
      "Action" : [
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "cloudfront:*",
        "cloudfront-keyvaluestore:*",
        "iam:ListServerCertificates",
        "waf:ListWebACLs",
        "waf:GetWebACL",
        "wafv2:ListWebACLs",
        "wafv2:GetWebACL",
        "kinesis:ListStreams",
        "ec2:DescribeInstances",
        "elasticloadbalancing:DescribeLoadBalancers",
        "ec2:DescribeInternetGateways"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:RequestCertificate"
      ],
      "Resource" : "*",
      "Sid" : "cfrequestcertificate",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "cloudfront.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "cffdescribestream",
```

```
      "Action" : [
        "kinesis:DescribeStream"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:kinesis:*:*:*"
    },
    {
      "Sid" : "cfflistroles",
      "Action" : [
        "iam:ListRoles"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

CloudFrontReadOnlyAccess

Deskripsi: Menyediakan akses ke informasi konfigurasi CloudFront distribusi dan daftar distribusi melalui. AWS Management Console

`CloudFrontReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudFrontReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:39 UTC

- Waktu yang telah diedit: 28 April 2025, 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/CloudFrontReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

CloudHSMServiceRolePolicy

Deskripsi: Mengaktifkan akses ke AWS sumber daya yang digunakan atau dikelola oleh CloudHSM

`CloudHSMServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 06 November 2017, 19:12 UTC
- Waktu telah diedit: 06 November 2017, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudHSMServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

CloudSearchFullAccess

Deskripsi: Menyediakan akses penuh ke layanan CloudSearch konfigurasi Amazon.

`CloudSearchFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudSearchFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:39 UTC
- Waktu telah diedit: 06 Februari 2015, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/CloudSearchFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

CloudSearchReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke layanan CloudSearch konfigurasi Amazon.

`CloudSearchReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudSearchReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:39 UTC
- Waktu telah diedit: 06 Februari 2015, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/CloudSearchReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

CloudTrailEventContext

Deskripsi: Peran terkait layanan ini memungkinkan CloudTrail untuk mendapatkan dan menambahkan tag sumber daya ke CloudTrail peristiwa pemilik sumber daya.

`CloudTrailEventContext`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 15 Mei 2025, 13:52 UTC
- Waktu yang telah diedit: 15 Mei 2025, 13:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudTrailEventContext`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

CloudTrailServiceRolePolicy

Deskripsi: Kebijakan izin untuk CloudTrail ServiceLinkedRole

`CloudTrailServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 24 Oktober 2018, 21:21 UTC
- Waktu telah diedit: November 27, 2023, 01:18 UTC

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

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudTrailFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AwsOrgsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AwsOrgsDelegatedAdminAccess",
      "Effect" : "Allow",
      "Action" : "organizations:ListDelegatedAdministrators",
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "cloudtrail.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DeleteTableAccess",
      "Effect" : "Allow",
      "Action" : "glue:DeleteTable",
      "Resource" : [
        "arn:*:glue:*:*:catalog",
        "arn:*:glue:*:*:database/aws:cloudtrail",
        "arn:*:glue:*:*:table/aws:cloudtrail/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DeregisterResourceAccess",
      "Effect" : "Allow",
      "Action" : "lakeformation:DeregisterResource",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

CloudWatch-CrossAccountAccess

Deskripsi: Memungkinkan CloudWatch untuk mengasumsikan CloudWatch - CrossAccountSharing peran dalam akun jarak jauh atas nama akun saat ini untuk menampilkan data lintas akun, lintas wilayah

`CloudWatch-CrossAccountAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 23 Juli 2019, 09:59 UTC
- Waktu yang telah diedit: 23 Juli 2019, 09:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatch-CrossAccountAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      "Resource" : [
        "arn:aws:iam::*:role/CloudWatch-CrossAccountSharing*"
      ],
      "Effect" : "Allow"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

CloudWatchActionsEC2Access

Deskripsi: Menyediakan akses hanya-baca ke CloudWatch alarm dan metrik serta metadata. EC2 Menyediakan akses ke EC2 instance Stop, Terminate, dan Reboot.

`CloudWatchActionsEC2Access`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchActionsEC2Access` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 07 Juli 2015, 00:00 UTC
- Waktu telah diedit: 07 Juli 2015, 00:00 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchActionsEC2Access`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:Describe*",
        "ec2:Describe*",
        "ec2:RebootInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

CloudWatchAgentAdminPolicy

Deskripsi: Izin penuh diperlukan untuk menggunakan AmazonCloudWatchAgent.

`CloudWatchAgentAdminPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchAgentAdminPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 07 Maret 2018, 00:52 UTC
- Waktu telah diedit: 05 Februari 2024, 20:59 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchAgentAdminPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CWACloudWatchPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData",
        "ec2:DescribeTags",
        "logs:PutLogEvents",
        "logs:PutRetentionPolicy",
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups",
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CWASSMPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ssm:GetParameter",
        "ssm:PutParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/AmazonCloudWatch-*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

CloudWatchAgentServerPolicy

Deskripsi: Izin yang diperlukan untuk digunakan AmazonCloudWatchAgent di server

`CloudWatchAgentServerPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchAgentServerPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 07 Maret 2018, 01:06 UTC
- Waktu telah diedit: 06 Februari 2024, 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchAgentServerPolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CWACloudWatchServerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData",
        "ec2:DescribeVolumes",
        "ec2:DescribeTags",
        "logs:PutLogEvents",
        "logs:PutRetentionPolicy",
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups",
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CWASSMServerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/AmazonCloudWatch-*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

CloudWatchApplicationInsightsFullAccess

Deskripsi: Menyediakan akses penuh ke Wawasan CloudWatch Aplikasi dan dependensi yang diperlukan.

`CloudWatchApplicationInsightsFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchApplicationInsightsFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 24 November 2020, 18:44 UTC
- Waktu yang telah diedit: 25 Januari 2022, 17.51 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchApplicationInsightsFullAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "applicationinsights:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "sqs:ListQueues",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "autoscaling:DescribeAutoScalingGroups",
        "lambda:ListFunctions",
        "dynamodb:ListTables",
        "s3:ListAllMyBuckets",
        "sns:ListTopics",
        "states:ListStateMachines",
        "apigateway:GET",
        "ecs:ListClusters",
        "ecs:DescribeTaskDefinition",
        "ecs:ListServices",
        "ecs:ListTasks",
        "eks:ListClusters",
        "eks:ListNodegroups",
        "fsx:DescribeFileSystems",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/application-insights.amazonaws.com/
AWSServiceRoleForApplicationInsights"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "application-insights.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

CloudWatchApplicationInsightsReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Wawasan CloudWatch Aplikasi.

`CloudWatchApplicationInsightsReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchApplicationInsightsReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 24 November 2020, 18:48 UTC
- Waktu yang telah diedit: 24 November 2020, 18:48 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchApplicationInsightsReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

CloudwatchApplicationInsightsServiceLinkedRolePolicy

Deskripsi: Kebijakan Peran Tertaut Layanan Wawasan Aplikasi Cloudwatch

`CloudwatchApplicationInsightsServiceLinkedRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 01 Desember 2018, 16:22 UTC
- Waktu yang telah diedit: 25 Juli 2024, 16:24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudwatchApplicationInsightsServiceLinkedRolePolicy`

Versi kebijakan

Versi kebijakan: v25 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM

- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

CloudWatchApplicationSignalsFullAccess

Deskripsi: Menyediakan akses penuh ke layanan Sinyal CloudWatch Aplikasi dan akses cakupan ke dependensi yang diperlukan untuk menggunakan dan mengoperasikan layanan ini.

`CloudWatchApplicationSignalsFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchApplicationSignalsFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Juni 2024, 22:50 UTC
- Waktu telah diedit: 06 Juni 2024, 22:50 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchApplicationSignalsFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchApplicationSignalsFullAccessPermissions",
      "Effect" : "Allow",
      "Action" : "application-signals:*",
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "CloudWatchApplicationSignalsAlarmsPermissions",
      "Effect" : "Allow",
      "Action" : "cloudwatch:DescribeAlarms",
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsMetricsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsLogGroupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:StartQuery"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/application-signals/data:*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsLogsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:StopQuery",
        "logs:GetQueryResults"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsSyntheticsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "synthetics:DescribeCanaries",
        "synthetics:DescribeCanariesLastRun",
        "synthetics:GetCanaryRuns"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "CloudWatchApplicationSignalsRumPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rum:BatchCreateRumMetricDefinitions",
        "rum:BatchDeleteRumMetricDefinitions",
        "rum:BatchGetRumMetricDefinitions",
        "rum:GetAppMonitor",
        "rum:GetAppMonitorData",
        "rum:ListAppMonitors",
        "rum:PutRumMetricsDestination",
        "rum:UpdateRumMetricDefinition"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsXrayPermissions",
      "Effect" : "Allow",
      "Action" : "xray:GetTraceSummaries",
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsPutMetricAlarmPermissions",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricAlarm",
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:SLO-AttainmentGoalAlarm-*",
        "arn:aws:cloudwatch:*:*:alarm:SLO-WarningAlarm-*",
        "arn:aws:cloudwatch:*:*:alarm:SLI-HealthAlarm-*"
      ]
    },
    {
      "Sid" : "CloudWatchApplicationSignalsCreateServiceLinkedRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/application-
signals.cloudwatch.amazonaws.com/AWSServiceRoleForCloudWatchApplicationSignals",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "application-signals.cloudwatch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchApplicationSignalsGetRolePermissions",
```

```
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/application-
signals.cloudwatch.amazonaws.com/AWSServiceRoleForCloudWatchApplicationSignals"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsSnsWritePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:Subscribe"
      ],
      "Resource" : "arn:aws:sns:*:*:cloudwatch-application-signals-*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsSnsReadPermissions",
      "Effect" : "Allow",
      "Action" : "sns:ListTopics",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

CloudWatchApplicationSignalsReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke layanan Sinyal CloudWatch Aplikasi dan akses cakupan ke dependensi yang diperlukan untuk menggunakan layanan ini

`CloudWatchApplicationSignalsReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchApplicationSignalsReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Juni 2024, 22:48 UTC
- Waktu telah diedit: 06 Juni 2024, 22:48 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchApplicationSignalsReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchApplicationSignalsReadOnlyAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "application-signals:BatchGetServiceLevelObjectiveBudgetReport",
        "application-signals:GetService",
        "application-signals:GetServiceLevelObjective",
        "application-signals:ListServiceLevelObjectives",
        "application-signals:ListServiceDependencies",
        "application-signals:ListServiceDependents",
        "application-signals:ListServiceOperations",
        "application-signals:ListServices",
        "application-signals:ListTagsForResource"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "CloudWatchApplicationSignalsGetRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/application-
signals.cloudwatch.amazonaws.com/AWSServiceRoleForCloudWatchApplicationSignals"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsLogGroupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:StartQuery"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/application-signals/data:*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsLogsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:StopQuery",
        "logs:GetQueryResults"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsAlarmsReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsMetricsReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsSyntheticsReadPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "synthetics:DescribeCanaries",
        "synthetics:DescribeCanariesLastRun",
        "synthetics:GetCanaryRuns"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsRumReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rum:BatchGetRumMetricDefinitions",
        "rum:GetAppMonitor",
        "rum:GetAppMonitorData",
        "rum:ListAppMonitors"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsXrayReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "xray:GetTraceSummaries"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

CloudWatchApplicationSignalsServiceRolePolicy

Deskripsi: Kebijakan memberikan izin kepada Sinyal CloudWatch Aplikasi untuk mengumpulkan data pemantauan dan penandaan dari layanan terkait AWS lainnya.

`CloudWatchApplicationSignalsServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 09 November 2023, 18:09 UTC
- Waktu yang telah diedit: 17 Maret 2025, 15:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchApplicationSignalsServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CWLogsPermission",
      "Effect" : "Allow",
      "Action" : [
        "logs:StartQuery",
        "logs:GetQueryResults"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/appsignals/*:*",
        "arn:aws:logs:*:*:log-group:/aws/application-signals/data:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${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}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

CloudWatchAutomaticDashboardsAccess

Deskripsi: Menyediakan akses ke yang tidak CloudWatch APIs digunakan untuk menampilkan Dasbor CloudWatch Otomatis, termasuk isi objek seperti fungsi Lambda

`CloudWatchAutomaticDashboardsAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchAutomaticDashboardsAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 23 Juli 2019, 10:01 UTC
- Waktu yang telah diedit: 20 April 2021, 13:05 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchAutomaticDashboardsAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "autoscaling:DescribeAutoScalingGroups",
        "cloudfront:GetDistribution",
        "cloudfront:ListDistributions",
        "dynamodb:DescribeTable",
        "dynamodb:ListTables",
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ecs:DescribeClusters",
        "ecs:DescribeContainerInstances",
        "ecs:ListClusters",
        "ecs:ListContainerInstances",
        "ecs:ListServices",
        "elasticache:DescribeCacheClusters",
        "elasticbeanstalk:DescribeEnvironments",
        "elasticfilesystem:DescribeFileSystems",
        "elasticloadbalancing:DescribeLoadBalancers",
        "kinesis:DescribeStream",
        "kinesis:ListStreams",
        "lambda:GetFunction",
        "lambda:ListFunctions",
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstances",
        "resource-groups:ListGroupResources",
        "resource-groups:ListGroups",
        "route53:GetHealthCheck",
        "route53:ListHealthChecks",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
```

```
        "sns:ListTopics",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ListQueues",
        "synthetics:DescribeCanariesLastRun",
        "tag:GetResources"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "apigateway:GET"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:apigateway:*::/restapis*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

CloudWatchCrossAccountSharingConfiguration

Deskripsi: Menyediakan kemampuan untuk mengelola tautan Observability Access Manager dan membangun pembagian CloudWatch sumber daya

`CloudWatchCrossAccountSharingConfiguration`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchCrossAccountSharingConfiguration` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 November 2022, 14:01 UTC
- Waktu yang telah diedit: 27 November 2022, 14.01 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchCrossAccountSharingConfiguration`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:Link",
        "oam:ListLinks"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:DeleteLink",
        "oam:GetLink",
        "oam:TagResource"
      ],
      "Resource" : "arn:aws:oam:*:*:link/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "oam:CreateLink",
        "oam:UpdateLink"
      ],
      "Resource" : [
        "arn:aws:oam:*:*:link/*",
        "arn:aws:oam:*:*:sink/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

CloudWatchEventsBuiltInTargetExecutionAccess

Deskripsi: Memungkinkan target bawaan di Amazon CloudWatch Events untuk melakukan EC2 tindakan atas nama Anda.

`CloudWatchEventsBuiltInTargetExecutionAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchEventsBuiltInTargetExecutionAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 14 Januari 2016, 18:35 UTC
- Waktu telah diedit: 14 Januari 2016, 18:35 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/CloudWatchEventsBuiltInTargetExecutionAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchEventsBuiltInTargetExecutionAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:Describe*",
        "ec2:RebootInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:CreateSnapshot"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

CloudWatchEventsFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon CloudWatch Events.

`CloudWatchEventsFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchEventsFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 14 Januari 2016, 18:37 UTC
- Waktu telah diedit: 22 Januari 2025, 02:07 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchEventsFullAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EventBridgeActions",
      "Effect" : "Allow",
      "Action" : [
        "events:*",
        "schemas:*",
        "scheduler:*",
        "pipes:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMCreateServiceLinkedRoleForApiDestinations",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
```

```
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
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"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

CloudWatchEventsInvocationAccess

Deskripsi: Memungkinkan CloudWatch Acara Amazon untuk menyampaikan peristiwa ke aliran di Aliran AWS Kinesis di akun Anda.

`CloudWatchEventsInvocationAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchEventsInvocationAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 14 Januari 2016, 18:36 UTC
- Waktu telah diedit: 14 Januari 2016, 18:36 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/CloudWatchEventsInvocationAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

CloudWatchEventsReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke CloudWatch Acara Amazon.

`CloudWatchEventsReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchEventsReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 14 Januari 2016, 18:27 UTC
- Waktu yang telah diedit: 01 Desember 2022, 16.29 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchEventsReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:DescribeEventBus",
        "events:DescribeEventSource",
        "events:ListEventBuses",
        "events:ListEventSources",
        "events:ListRuleNamesByTarget",
```

```
        "events:ListRules",
        "events:ListTargetsByRule",
        "events:TestEventPattern",
        "events:DescribeArchive",
        "events:ListArchives",
        "events:DescribeReplay",
        "events:ListReplays",
        "events:DescribeConnection",
        "events:ListConnections",
        "events:DescribeApiDestination",
        "events:ListApiDestinations",
        "events:DescribeEndpoint",
        "events:ListEndpoints",
        "schemas:DescribeCodeBinding",
        "schemas:DescribeDiscoverer",
        "schemas:DescribeRegistry",
        "schemas:DescribeSchema",
        "schemas:ExportSchema",
        "schemas:GetCodeBindingSource",
        "schemas:GetDiscoveredSchema",
        "schemas:GetResourcePolicy",
        "schemas:ListDiscoverers",
        "schemas:ListRegistries",
        "schemas:ListSchemas",
        "schemas:ListSchemaVersions",
        "schemas:ListTagsForResource",
        "schemas:SearchSchemas",
        "scheduler:GetSchedule",
        "scheduler:GetScheduleGroup",
        "scheduler:ListSchedules",
        "scheduler:ListScheduleGroups",
        "scheduler:ListTagsForResource",
        "pipes:DescribePipe",
        "pipes:ListPipes",
        "pipes:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

CloudWatchEventsServiceRolePolicy

Deskripsi: Izinkan AWS CloudWatch untuk menjalankan tindakan atas nama Anda yang dikonfigurasi melalui alarm dan acara.

`CloudWatchEventsServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 17 November 2017, 00:42 UTC
- Waktu diedit: 17 November 2017, 00:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchEventsServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

CloudWatchFullAccess

Deskripsi: Menyediakan akses penuh ke CloudWatch.

`CloudWatchFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu yang telah diedit: 27 November 2022, 13.23 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchFullAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:Describe*",
        "cloudwatch:*",
        "logs:*",
        "sns:*",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "oam:ListSinks"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/events.amazonaws.com/
AWSServiceRoleForCloudWatchEvents*",
      "Condition" : {
```

```
        "StringLike" : {
          "iam:AWSServiceName" : "events.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:ListAttachedLinks"
      ],
      "Resource" : "arn:aws:oam:*:*:sink/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

CloudWatchFullAccessV2

Deskripsi: Menyediakan akses penuh ke CloudWatch.

`CloudWatchFullAccessV2`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchFullAccessV2` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Agustus 2023, 11:32 UTC
- Waktu yang telah diedit: 17 Mei 2024, 22:20 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchFullAccessV2`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchFullAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalingPolicies",
        "application-signals:*",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribePolicies",
        "cloudwatch:*",
        "logs:*",
        "sns:CreateTopic",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "sns:Subscribe",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "oam:ListSinks",
        "rum:*",
        "synthetics:*",
        "xray:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsServiceLinkedRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
```

```
      "Resource" : "arn:aws:iam::*:role/aws-service-role/application-
signals.cloudwatch.amazonaws.com/AWSServiceRoleForCloudWatchApplicationSignals",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "application-signals.cloudwatch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EventsServicePermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/events.amazonaws.com/
AWSServiceRoleForCloudWatchEvents*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "events.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "OAMReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "oam:ListAttachedLinks"
      ],
      "Resource" : "arn:aws:oam:*:*:sink/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

CloudWatchInternetMonitorFullAccess

Deskripsi: Menyediakan akses penuh ke tindakan untuk bekerja dengan Amazon CloudWatch Internet Monitor. Juga menyediakan akses ke layanan lain, seperti Amazon CloudWatch, Amazon, Amazon EC2, Amazon CloudFront WorkSpaces, dan Elastic Load Balancing, yang diperlukan untuk menggunakan layanan Internet Monitor untuk memantau dan menyimpan informasi tentang lalu lintas aplikasi.

`CloudWatchInternetMonitorFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchInternetMonitorFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 22 Oktober 2024, 21:02 UTC
- Waktu telah diedit: 22 Oktober 2024, 21:02 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchInternetMonitorFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

CloudWatchInternetMonitorReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke tindakan untuk bekerja dengan Amazon CloudWatch Internet Monitor. Juga menyediakan akses ke layanan lain di Amazon CloudWatch, termasuk kebijakan untuk mengambil informasi tentang CloudWatch metrik dan untuk mengelola kueri log, yang diperlukan untuk menggunakan layanan Internet Monitor untuk memantau dan menyimpan informasi tentang lalu lintas aplikasi.

`CloudWatchInternetMonitorReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchInternetMonitorReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 12 November 2024, 23:11 UTC
- Waktu telah diedit: 12 November 2024, 23:11 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchInternetMonitorReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

CloudWatchInternetMonitorServiceRolePolicy

Deskripsi: Memungkinkan Internet Monitor untuk mengakses EC2, Ruang Kerja, dan CloudFront sumber daya, dan layanan lain yang diperlukan atas nama Anda.

`CloudWatchInternetMonitorServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 27 November 2022, 17:46 UTC
- Waktu telah diedit: 20 Juli 2023, 04:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchInternetMonitorServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:GetDistribution",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:DescribeLoadBalancers",
        "workspaces:DescribeWorkspaceDirectories"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:CreateLogGroup",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/internet-monitor/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/internet-monitor/*:log-stream:*"
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Condition" : {
        "StringEquals" : {
```

```
          "cloudwatch:namespace" : "AWS/InternetMonitor"
        }
      },
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

CloudWatchLambdaApplicationSignalsExecutionRolePolicy

Deskripsi: Menyediakan akses tulis ke grup log Sinyal X-Ray dan Sinyal CloudWatch Aplikasi.

`CloudWatchLambdaApplicationSignalsExecutionRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchLambdaApplicationSignalsExecutionRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 16 Oktober 2024, 19:09 UTC
- Waktu yang telah diedit: 16 Oktober 2024, 19:09 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLambdaApplicationSignalsExecutionRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

CloudWatchLambdaInsightsExecutionRolePolicy

Deskripsi: Kebijakan yang diperlukan untuk Ekstensi Wawasan Lambda

`CloudWatchLambdaInsightsExecutionRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchLambdaInsightsExecutionRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 07 Oktober 2020, 19:27 UTC
- Waktu yang telah diedit: 07 Oktober 2020, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLambdaInsightsExecutionRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "logs:CreateLogGroup",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/lambda-insights:*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

CloudWatchLogsCrossAccountSharingConfiguration

Deskripsi: Menyediakan kemampuan untuk mengelola tautan Observability Access Manager dan membangun berbagi sumber daya CloudWatch Log

`CloudWatchLogsCrossAccountSharingConfiguration`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchLogsCrossAccountSharingConfiguration` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 27 November 2022, 13:55 UTC
- Waktu yang telah diedit: 27 November 2022, 13.55 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLogsCrossAccountSharingConfiguration`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:Link",
        "oam:ListLinks"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:DeleteLink",
        "oam:GetLink",
        "oam:TagResource"
      ],
      "Resource" : "arn:aws:oam:*:*:link/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:CreateLink",
        "oam:UpdateLink"
```

```
      ],
      "Resource" : [
        "arn:aws:oam:*:*:link/*",
        "arn:aws:oam:*:*:sink/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

CloudWatchLogsFullAccess

Deskripsi: Menyediakan akses penuh ke CloudWatch Log

`CloudWatchLogsFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchLogsFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu yang telah diedit: 20 Mei 2025, 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLogsFullAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchLogsFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:*",
        "cloudwatch:GenerateQuery",
        "cloudwatch:GenerateQueryResultsSummary"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

CloudWatchLogsReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke CloudWatch Log

`CloudWatchLogsReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchLogsReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu yang telah diedit: 20 Mei 2025, 16:52 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLogsReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchLogsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:Describe*",
        "logs:Get*",
        "logs:List*",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:TestMetricFilter",
        "logs:FilterLogEvents",
        "logs:StartLiveTail",
        "logs:StopLiveTail",
        "cloudwatch:GenerateQuery",
        "cloudwatch:GenerateQueryResultsSummary"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

CloudWatchNetworkFlowMonitorAgentPublishPolicy

Deskripsi: Anda dapat menggunakan kebijakan ini dalam peran IAM yang dilampirkan ke sumber daya instans Amazon EC2 dan Amazon EKS untuk mengirim laporan telemetri (metrik) ke titik akhir Network Flow Monitor.

`CloudWatchNetworkFlowMonitorAgentPublishPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchNetworkFlowMonitorAgentPublishPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Desember 2024, 22:51 UTC
- Waktu yang telah diedit: 01 Desember 2024, 22:51 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchNetworkFlowMonitorAgentPublishPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

CloudWatchNetworkFlowMonitorServiceRolePolicy

Deskripsi: Anda tidak dapat melampirkan CloudWatchNetworkFlowMonitorServiceRolePolicy ke entitas IAM Anda. Kebijakan ini dilampirkan pada peran terkait layanan bernama AWSServiceRoleForNetworkFlowMonitor, yang menerbitkan hasil agregasi telemetri jaringan, yang dikumpulkan oleh agen Network Flow Monitor, ke. CloudWatch Ini juga memungkinkan layanan untuk menggunakan AWS Organizations untuk mendapatkan informasi untuk skenario multi-akun.

`CloudWatchNetworkFlowMonitorServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 01 Desember 2024, 22:36 UTC
- Waktu yang telah diedit: 29 April 2025, 10:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchNetworkFlowMonitorServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

CloudWatchNetworkFlowMonitorTopologyServiceRolePolicy

Deskripsi: Anda tidak dapat melampirkan CloudWatchNetworkFlowMonitorTopologyServiceRolePolicy ke entitas IAM Anda. Kebijakan ini dilampirkan ke peran terkait layanan bernama AWSServiceRoleForNetworkFlowMonitor_Topology, yang menghasilkan snapshot topologi sumber daya yang digunakan oleh Network Flow Monitor di akun Anda.

`CloudWatchNetworkFlowMonitorTopologyServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan

- Waktu pembuatan: 01 Desember 2024, 22:51 UTC
- Waktu yang telah diedit: 01 Desember 2024, 22:51 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchNetworkFlowMonitorTopologyServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

CloudWatchNetworkMonitorServiceRolePolicy

Deskripsi: Memungkinkan Monitor CloudWatch Jaringan untuk mengakses dan mengelola EC2 dan sumber daya VPC, mempublikasikan data ke CloudWatch dan mengakses layanan lain yang diperlukan atas nama Anda.

`CloudWatchNetworkMonitorServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 21 Desember 2023, 18:53 UTC
- Waktu yang telah diedit: 21 Desember 2023, 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchNetworkMonitorServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PublishCw",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/NetworkMonitor"
        }
      }
    },
    {
      "Sid" : "DescribeAny",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DeleteModifyEc2Resources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
```

```
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/ManagedByCloudWatchNetworkMonitor" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

CloudWatchOpenSearchDashboardAccess

Deskripsi: Kebijakan ini menyediakan akses pengguna untuk melihat OpenSearch dasbor di konsol CloudWatch Log.

`CloudWatchOpenSearchDashboardAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchOpenSearchDashboardAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Desember 2024, 21:06 UTC
- Waktu yang telah diedit: 01 Desember 2024, 21:06 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchOpenSearchDashboardAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

CloudWatchOpenSearchDashboardsFullAccess

Deskripsi: Kebijakan ini menyediakan akses pengguna untuk membuat integrasi dengan OpenSearch membuat, memperbarui, menghapus, atau melihat dasbor di konsol CloudWatch Log.

`CloudWatchOpenSearchDashboardsFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchOpenSearchDashboardsFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Desember 2024, 21:06 UTC
- Waktu yang telah diedit: 01 Desember 2024, 21:06 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchOpenSearchDashboardsFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

CloudWatchReadOnlyAccess

Deskripsi: Menyediakan akses hanya baca ke CloudWatch.

`CloudWatchReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu telah diedit: 21 November 2024, 17:51 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v10 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchReadOnlyAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalingPolicies",
        "application-signals:BatchGet*",
        "application-signals:Get*",
        "application-signals:List*",
        "autoscaling:Describe*",
        "cloudwatch:BatchGet*",
        "cloudwatch:Describe*",
        "cloudwatch:GenerateQuery",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "logs:Get*",
        "logs:List*",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:Describe*",
        "logs:TestMetricFilter",
        "logs:FilterLogEvents",
        "logs:StartLiveTail",
        "logs:StopLiveTail",
        "oam:ListSinks",
        "sns:Get*",
        "sns:List*",
        "rum:BatchGet*",
        "rum:Get*",
        "rum:List*",
        "synthetics:Describe*",
```

```
        "synthetics:Get*",
        "synthetics:List*",
        "xray:BatchGet*",
        "xray:Get*",
        "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"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

CloudWatchSyntheticsFullAccess

Deskripsi: Menyediakan akses penuh ke CloudWatch Synthetics.

`CloudWatchSyntheticsFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchSyntheticsFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 25 November 2019, 17:39 UTC
- Waktu telah diedit: November 21, 2024, 22:21 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchSyntheticsFullAccess`

Versi kebijakan

Versi kebijakan: v11 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "synthetics:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutEncryptionConfiguration"
      ],
      "Resource" : [
        "arn:aws:s3:::cw-syn-results-*"
```

```
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "s3:ListAllMyBuckets",
        "xray:GetTraceSummaries",
        "xray:BatchGetTraces",
        "apigateway:GET"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::cw-syn-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::aws-synthetics-library-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/CloudWatchSyntheticsRole*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "iam:PassedToService" : [
            "lambda.amazonaws.com",
            "synthetics.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/CloudWatchSyntheticsRole*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:Synthetics-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:*"
      ]
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "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"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

CloudWatchSyntheticsReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke CloudWatch Synthetics.

`CloudWatchSyntheticsReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchSyntheticsReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 25 November 2019, 17:45 UTC
- Waktu yang telah diedit: 06 Maret 2020, 19:26 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchSyntheticsReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

ComprehendDataAccessRolePolicy

Deskripsi: Kebijakan untuk AWS Memahami peran layanan yang memungkinkan akses ke sumber daya S3 untuk akses data

`ComprehendDataAccessRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ComprehendDataAccessRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 06 Maret 2019, 22:28 UTC
- Waktu yang telah diedit: 06 Maret 2019, 22:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ComprehendDataAccessRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "s3:GetObject",
      "s3:ListBucket",
      "s3:PutObject"
    ],
    "Resource" : [
      "arn:aws:s3:::*Comprehend*",
      "arn:aws:s3:::*comprehend*"
    ]
  }
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

ComprehendFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Comprehend.

`ComprehendFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ComprehendFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 November 2017, 18:08 UTC
- Waktu telah diedit: 05 Desember 2017, 01:36 UTC
- ARN: `arn:aws:iam::aws:policy/ComprehendFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "comprehend:*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "iam:ListRoles",
        "iam:GetRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

ComprehendMedicalFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Comprehend Medical

`ComprehendMedicalFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ComprehendMedicalFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 November 2018, 17:55 UTC
- Waktu telah diedit: 27 November 2018, 17:55 UTC
- ARN: `arn:aws:iam::aws:policy/ComprehendMedicalFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

ComprehendReadOnly

Deskripsi: Menyediakan akses hanya-baca ke Amazon Comprehend.

`ComprehendReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ComprehendReadOnly` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 November 2017, 18:10 UTC
- Waktu yang telah diedit: 26 April 2022, 21.32 UTC
- ARN: `arn:aws:iam::aws:policy/ComprehendReadOnly`

Versi kebijakan

Versi kebijakan: v11 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "comprehend:DetectDominantLanguage",
        "comprehend:BatchDetectDominantLanguage",
        "comprehend:DetectEntities",
        "comprehend:BatchDetectEntities",
```

```
        "comprehend:DetectKeyPhrases",
        "comprehend:BatchDetectKeyPhrases",
        "comprehend:DetectPiiEntities",
        "comprehend:ContainsPiiEntities",
        "comprehend:DetectSentiment",
        "comprehend:BatchDetectSentiment",
        "comprehend:DetectSyntax",
        "comprehend:BatchDetectSyntax",
        "comprehend:ClassifyDocument",
        "comprehend:DescribeTopicsDetectionJob",
        "comprehend:ListTopicsDetectionJobs",
        "comprehend:DescribeDominantLanguageDetectionJob",
        "comprehend:ListDominantLanguageDetectionJobs",
        "comprehend:DescribeEntitiesDetectionJob",
        "comprehend:ListEntitiesDetectionJobs",
        "comprehend:DescribeKeyPhrasesDetectionJob",
        "comprehend:ListKeyPhrasesDetectionJobs",
        "comprehend:DescribePiiEntitiesDetectionJob",
        "comprehend:ListPiiEntitiesDetectionJobs",
        "comprehend:DescribeSentimentDetectionJob",
        "comprehend:DescribeTargetedSentimentDetectionJob",
        "comprehend:ListSentimentDetectionJobs",
        "comprehend:ListTargetedSentimentDetectionJobs",
        "comprehend:DescribeDocumentClassifier",
        "comprehend:ListDocumentClassifiers",
        "comprehend:DescribeDocumentClassificationJob",
        "comprehend:ListDocumentClassificationJobs",
        "comprehend:DescribeEntityRecognizer",
        "comprehend:ListEntityRecognizers",
        "comprehend:ListTagsForResource",
        "comprehend:DescribeEndpoint",
        "comprehend:ListEndpoints",
        "comprehend:ListDocumentClassifierSummaries",
        "comprehend:ListEntityRecognizerSummaries",
        "comprehend:DescribeResourcePolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

ComputeOptimizerReadOnlyAccess

Deskripsi: Menyediakan akses hanya baca ke ComputeOptimizer.

`ComputeOptimizerReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ComputeOptimizerReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 07 Maret 2020, 00:11 UTC
- Waktu telah diedit: 20 November 2024, 21:08 UTC
- ARN: `arn:aws:iam::aws:policy/ComputeOptimizerReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

ComputeOptimizerServiceRolePolicy

Deskripsi: Memungkinkan ComputeOptimizer untuk menelepon AWS layanan dan mengumpulkan rincian beban kerja atas nama Anda.

`ComputeOptimizerServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 03 Desember 2019, 08:45 UTC
- Waktu telah diedit: 03 Januari 2025, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ComputeOptimizerServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

ConfigConformsServiceRolePolicy

Deskripsi: Kebijakan yang diperlukan AWSConfig untuk membuat paket kesesuaian

`ConfigConformsServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 25 Juli 2019, 21:38 UTC
- Waktu telah diedit: 12 Januari 2023, 04:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ConfigConformsServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "config:PutConfigRule",
        "config:DeleteConfigRule"
      ],
      "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/config-
conforms.amazonaws.com*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigRules"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeRemediationConfigurations",
        "config:DeleteRemediationConfiguration",
        "config:PutRemediationConfigurations"
      ],
      "Resource" : "arn:aws:config:*:*:remediation-configuration/aws-service-
remediation-configuration/config-conforms.amazonaws.com*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
```

```
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/config-conforms.amazonaws.com/
*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
remediation.config.amazonaws.com/AWSServiceRoleForConfigRemediation"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
remediation.config.amazonaws.com/AWSServiceRoleForConfigRemediation",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "remediation.config.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument",
        "ssm:GetDocument"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:GetObject",
        "s3:GetBucketAcl"
      ],
      "Resource" : "arn:aws:s3:::awsconfigconforms*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:GetStackPolicy",
        "cloudformation:SetStackPolicy",
        "cloudformation:UpdateStack",
        "cloudformation:UpdateTerminationProtection",
        "cloudformation:ValidateTemplate",
        "cloudformation:ListStackResources"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/awsconfigconforms-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Config"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM

- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

CostOptimizationHubAdminAccess

Deskripsi: Kebijakan terkelola ini menyediakan akses admin ke Hub Pengoptimalan Biaya.

`CostOptimizationHubAdminAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CostOptimizationHubAdminAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 19 Desember 2023, 00:03 UTC
- Waktu yang telah diedit: 19 Desember 2023, 00:03 UTC
- ARN: `arn:aws:iam::aws:policy/CostOptimizationHubAdminAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CostOptimizationHubAdminAccess",
      "Effect" : "Allow",
      "Action" : [
        "cost-optimization-hub:ListEnrollmentStatuses",
        "cost-optimization-hub:UpdateEnrollmentStatus",
```

```
        "cost-optimization-hub:GetPreferences",
        "cost-optimization-hub:UpdatePreferences",
        "cost-optimization-hub:GetRecommendation",
        "cost-optimization-hub:ListRecommendations",
        "cost-optimization-hub:ListRecommendationSummaries"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCreationOfServiceLinkedRoleForCostOptimizationHub",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/cost-optimization-hub.bcm.amazonaws.com/
AWSServiceRoleForCostOptimizationHub"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "cost-optimization-hub.bcm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowAWSServiceAccessForCostOptimizationHub",
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "organizations:ServicePrincipal" : [
            "cost-optimization-hub.bcm.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

CostOptimizationHubReadOnlyAccess

Deskripsi: Kebijakan terkelola ini menyediakan akses hanya-baca ke Hub Pengoptimalan Biaya.

`CostOptimizationHubReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CostOptimizationHubReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 13 Desember 2023, 18:04 UTC
- Waktu yang telah diedit: 13 Desember 2023, 18:04 UTC
- ARN: `arn:aws:iam::aws:policy/CostOptimizationHubReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
  "Statement" : [
    {
      "Sid" : "CostOptimizationHubReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "cost-optimization-hub:ListEnrollmentStatuses",
        "cost-optimization-hub:GetPreferences",
        "cost-optimization-hub:GetRecommendation",
        "cost-optimization-hub:ListRecommendations",
        "cost-optimization-hub:ListRecommendationSummaries"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

CostOptimizationHubServiceRolePolicy

Deskripsi: Memungkinkan Hub Pengoptimalan Biaya untuk mengambil informasi organisasi dan mengumpulkan data dan metadata terkait pengoptimalan.

`CostOptimizationHubServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan

- Waktu pembuatan: 26 November 2023, 08:03 UTC
- Waktu telah diedit: 05 Juli 2024, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CostOptimizationHubServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

CustomerProfilesServiceLinkedRolePolicy

Deskripsi: Memungkinkan Profil Pelanggan Amazon Connect mengakses AWS layanan dan sumber daya atas nama Anda.

`CustomerProfilesServiceLinkedRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan

- Waktu pembuatan: 07 Maret 2023, 22:56 UTC
- Waktu telah diedit: 26 November 2024, 22:21 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CustomerProfilesServiceLinkedRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

DatabaseAdministrator

Deskripsi: Memberikan izin akses penuh ke AWS layanan dan tindakan yang diperlukan untuk menyiapkan dan mengonfigurasi layanan AWS basis data.

`DatabaseAdministrator`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `DatabaseAdministrator` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan fungsi Job
- Waktu pembuatan: 10 November 2016, 17:25 UTC
- Waktu yang telah diedit: 08 Januari 2019, 00:48 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/DatabaseAdministrator`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:Describe*",
        "cloudwatch:DisableAlarmActions",
        "cloudwatch:EnableAlarmActions",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "cloudwatch:PutMetricAlarm",
        "datapipeline:ActivatePipeline",
        "datapipeline:CreatePipeline",
        "datapipeline:DeletePipeline",
        "datapipeline:DescribeObjects",
        "datapipeline:DescribePipelines",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:ListPipelines",
        "datapipeline:PutPipelineDefinition",
        "datapipeline:QueryObjects",
        "dynamodb:*",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "elasticache:*",
        "iam:ListRoles",
        "iam:GetRole",
```

```
        "kms:ListKeys",
        "lambda:CreateEventSourceMapping",
        "lambda:CreateFunction",
        "lambda:DeleteEventSourceMapping",
        "lambda:DeleteFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:ListEventSourceMappings",
        "lambda:ListFunctions",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:FilterLogEvents",
        "logs:GetLogEvents",
        "logs:Create*",
        "logs:PutLogEvents",
        "logs:PutMetricFilter",
        "rds:*",
        "redshift:*",
        "s3:CreateBucket",
        "sns:CreateTopic",
        "sns:DeleteTopic",
        "sns:Get*",
        "sns:List*",
        "sns:SetTopicAttributes",
        "sns:Subscribe",
        "sns:Unsubscribe"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject*",
        "s3:Get*",
        "s3:List*",
        "s3:PutAccelerateConfiguration",
        "s3:PutBucketTagging",
        "s3:PutBucketVersioning",
        "s3:PutBucketWebsite",
        "s3:PutLifecycleConfiguration",
        "s3:PutReplicationConfiguration",
        "s3:PutObject*",
        "s3:Replicate*",
        "s3:RestoreObject"
```

```
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/rds-monitoring-role",
        "arn:aws:iam::*:role/rdbms-lambda-access",
        "arn:aws:iam::*:role/lambda_exec_role",
        "arn:aws:iam::*:role/lambda-dynamodb-*",
        "arn:aws:iam::*:role/lambda-vpc-execution-role",
        "arn:aws:iam::*:role/DataPipelineDefaultRole",
        "arn:aws:iam::*:role/DataPipelineDefaultResourceRole"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

DataScientist

Deskripsi: Memberikan izin ke layanan analisis AWS data.

`DataScientist`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `DataScientist` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan fungsi Job
- Waktu pembuatan: 10 November 2016, 17:28 UTC
- Waktu diedit: 03 Desember 2019, 16:48 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/DataScientist`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "autoscaling:*",
        "cloudwatch:*",
        "cloudformation:CreateStack",
        "cloudformation:DescribeStackEvents",
        "datapipeline:Describe*",
        "datapipeline:ListPipelines",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:QueryObjects",
        "dynamodb:*",
        "ec2:CancelSpotInstanceRequests",
        "ec2:CancelSpotFleetRequests",
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "ec2:Describe*",
        "ec2:ModifyImageAttribute",
        "ec2:ModifyInstanceAttribute",
        "ec2:ModifySpotFleetRequest",
        "ec2:RequestSpotInstances",
```

```
        "ec2:RequestSpotFleet",
        "elasticfilesystem:*",
        "elasticmapreduce:*",
        "es:*",
        "firehose:*",
        "fsx:DescribeFileSystems",
        "iam:GetInstanceProfile",
        "iam:GetRole",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:ListRoles",
        "kinesis:*",
        "kms:List*",
        "lambda:Create*",
        "lambda:Delete*",
        "lambda:Get*",
        "lambda:InvokeFunction",
        "lambda:PublishVersion",
        "lambda:Update*",
        "lambda:List*",
        "machinelearning:*",
        "sdb:*",
        "rds:*",
        "sns:ListSubscriptions",
        "sns:ListTopics",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "redshift:*",
        "s3:CreateBucket",
        "sns:CreateTopic",
        "sns:Get*",
        "sns:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:Abort*",
        "s3:DeleteObject",
        "s3:Get*",
        "s3:List*",
        "s3:PutAccelerateConfiguration",
```

```
        "s3:PutBucketCors",
        "s3:PutBucketLogging",
        "s3:PutBucketNotification",
        "s3:PutBucketTagging",
        "s3:PutObject",
        "s3:Replicate*",
        "s3:RestoreObject"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/DataPipelineDefaultRole",
        "arn:aws:iam::*:role/DataPipelineDefaultResourceRole",
        "arn:aws:iam::*:role/EMR_EC2_DefaultRole",
        "arn:aws:iam::*:role/EMR_DefaultRole",
        "arn:aws:iam::*:role/kinesis-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "sagemaker.amazonaws.com"
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:*"
      ],
      "NotResource" : [
        "arn:aws:sagemaker:*:*:domain/*",
        "arn:aws:sagemaker:*:*:user-profile/*",
        "arn:aws:sagemaker:*:*:app/*",
        "arn:aws:sagemaker:*:*:flow-definition/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreatePresignedDomainUrl",
        "sagemaker:DescribeDomain",
        "sagemaker:ListDomains",
        "sagemaker:DescribeUserProfile",
        "sagemaker:ListUserProfiles",
        "sagemaker:*App",
        "sagemaker:ListApps"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:*FlowDefinition",
        "sagemaker:*FlowDefinitions"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "sagemaker:WorkteamType" : [
            "private-crowd",
            "vendor-crowd"
          ]
        }
      }
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

DAXServiceRolePolicy

Deskripsi: Kebijakan ini memungkinkan DAX untuk membuat dan mengelola antarmuka Jaringan, grup Keamanan, Subnet, dan Vpc atas nama pelanggan

`DAXServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 05 Maret 2018, 17:51 UTC
- Waktu telah diedit: 05 Maret 2018, 17:51 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DAXServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

DeclarativePoliciesEC2Report

Deskripsi: Menyediakan akses ke read-only yang APIs diperlukan untuk menjalankan Kebijakan EC2 Deklaratif Laporan Status Akun.

`DeclarativePoliciesEC2Report`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 30 November 2024, 13:21 UTC
- Waktu telah diedit: 30 November 2024, 13:21 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DeclarativePoliciesEC2Report`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

DynamoDBCloudWatchContributorInsightsServiceRolePolicy

Deskripsi: Izin diperlukan untuk mendukung Amazon CloudWatch Contributor Insights untuk Amazon DynamoDB.

`DynamoDBCloudWatchContributorInsightsServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 15 November 2019, 21:13 UTC
- Waktu yang telah diedit: 15 November 2019, 21:13 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DynamoDBCloudWatchContributorInsightsServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudwatch:DeleteInsightRules",
        "cloudwatch:PutInsightRule"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:cloudwatch:*:*:insight-rule/DynamoDBContributorInsights*"
    },
    {
      "Action" : [
        "cloudwatch:DescribeInsightRules"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

DynamoDBKinesisReplicationServiceRolePolicy

Deskripsi: Menyediakan akses AWS DynamoDB ke KinesisDataStreams

`DynamoDBKinesisReplicationServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 12 November 2020 00:43 UTC
- Waktu yang telah diedit: 12 November 2020, 00:43 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DynamoDBKinesisReplicationServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "kms:GenerateDataKey",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "kinesis.*.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "kinesis:PutRecord",
        "kinesis:PutRecords",
        "kinesis:DescribeStream"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

DynamoDBReplicationServiceRolePolicy

Deskripsi: Izin yang diperlukan oleh DynamoDB untuk replikasi data lintas wilayah

`DynamoDBReplicationServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 09 November 2017, 23:55 UTC
- Waktu telah diedit: 08 Januari 2024, 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DynamoDBReplicationServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DynamoDBActionsNeededForSteadyStateReplication",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:GetItem",
        "dynamodb:PutItem",
        "dynamodb:UpdateItem",
        "dynamodb:DeleteItem",
        "dynamodb:DescribeTable",
        "dynamodb:UpdateTable",
        "dynamodb:Scan",
        "dynamodb:DescribeStream",
        "dynamodb:GetRecords",
        "dynamodb:GetShardIterator",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:UpdateTimeToLive",
        "dynamodb:DescribeLimits",
        "dynamodb:GetResourcePolicy",
        "application-autoscaling:RegisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:DescribeScalingPolicies",
        "account:ListRegions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DynamoDBReplicationServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "dynamodb.application-autoscaling.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

EC2FastLaunchFullAccess

Deskripsi: Kebijakan ini memberikan akses penuh ke tindakan Peluncuran EC2 Cepat

`EC2FastLaunchFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `EC2FastLaunchFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 13 Mei 2024, 22:45 UTC
- Waktu yang telah diedit: 14 Mei 2025, 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/EC2FastLaunchFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

EC2FastLaunchServiceRolePolicy

Deskripsi: Kebijakan memberikan ec2fastlaunch untuk menyiapkan dan mengelola snapshot yang telah disediakan sebelumnya di akun pelanggan & mempublikasikan metrik terkait.

`EC2FastLaunchServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 10 Januari 2022, 13:08 UTC
- Waktu yang telah diedit: 14 Mei 2025, 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/EC2FastLaunchServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "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" : "AllowDescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "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"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

EC2FleetTimeShiftableServiceRolePolicy

Deskripsi: Kebijakan yang memberikan izin kepada EC2 Armada untuk meluncurkan instans di masa mendatang.

`EC2FleetTimeShiftableServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 23 Desember 2019 19:47 UTC
- Waktu yang telah diedit: 23 Desember 2019, 19:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/EC2FleetTimeShiftableServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

Ec2ImageBuilderCrossAccountDistributionAccess

Deskripsi: Izin yang diperlukan oleh EC2 Image Builder untuk melakukan distribusi lintas akun.

`Ec2ImageBuilderCrossAccountDistributionAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `Ec2ImageBuilderCrossAccountDistributionAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 September 2020 19:22 UTC

- Waktu yang telah diedit: 30 September 2020, 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/Ec2ImageBuilderCrossAccountDistributionAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*::image/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:CopyImage",
        "ec2:ModifyImageAttribute"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

EC2ImageBuilderLifecycleExecutionPolicy

Deskripsi: EC2 ImageBuilderLifecycleExecutionPolicy Kebijakan ini memberikan izin bagi Image Builder untuk melakukan tindakan seperti menghentikan atau menghapus sumber daya gambar Image Builder dan sumber daya dasarnya (AMIssnapshot) guna mendukung aturan otomatis untuk tugas pengelolaan siklus hidup gambar.

`EC2ImageBuilderLifecycleExecutionPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `EC2ImageBuilderLifecycleExecutionPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 16 November 2023, 23:23 UTC
- Waktu telah diedit: 16 November 2023, 23:23 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/EC2ImageBuilderLifecycleExecutionPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      "Sid" : "Ec2ImagePermission",
      "Effect" : "Allow",
      "Action" : [
        "ec2:EnableImage",
        "ec2:DeregisterImage",
        "ec2:EnableImageDeprecation",
        "ec2:DescribeImageAttribute",
        "ec2:DisableImage",
        "ec2:DisableImageDeprecation"
      ],
      "Resource" : "arn:aws:ec2:*::image/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "EC2DeleteSnapshotPermission",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteSnapshot",
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "EC2TagsPermission",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteTags",
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*::image/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/DeprecatedBy" : "EC2 Image Builder",
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        },
```

```
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "DeprecatedBy"
        }
      }
    },
    {
      "Sid" : "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" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

EC2InstanceConnect

Deskripsi: Memungkinkan pelanggan memanggil EC2 Instance Connect untuk mempublikasikan kunci singkat ke EC2 instans mereka dan terhubung melalui ssh atau CLI Instance Connect EC2 .

`EC2InstanceConnect`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `EC2InstanceConnect` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Juni 2019, 18:53 UTC
- Waktu yang telah diedit: 27 Juni 2019, 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/EC2InstanceConnect`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2InstanceConnect",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2-instance-connect:SendSSHPublicKey"
      ],
      "Effect" : "Allow",
```

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

Ec2InstanceConnectEndpoint

Deskripsi: Kebijakan titik akhir EC2 Instance Connect untuk mengelola titik akhir EC2 Instance Connect yang dibuat oleh pelanggan

`Ec2InstanceConnectEndpoint`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 24 Januari 2023, 20:19 UTC
- Waktu telah diedit: 24 Januari 2023, 20:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Ec2InstanceConnectEndpoint`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:subnet/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "InstanceConnectEndpointId"
          ]
        },
        "Null" : {
          "aws:RequestTag/InstanceConnectEndpointId" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/InstanceConnectEndpointId" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "InstanceConnectEndpointId"
          ]
        },
        "Null" : {
          "aws:RequestTag/InstanceConnectEndpointId" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/InstanceConnectEndpointId" : [
            "eice-*"
          ]
        }
      }
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

EC2InstanceProfileForImageBuilder

Deskripsi: Profil EC2 instance untuk layanan Image Builder.

`EC2InstanceProfileForImageBuilder`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `EC2InstanceProfileForImageBuilder` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Desember 2019, 19:08 UTC
- Waktu telah diedit: 19 Mei 2025, 20:37 UTC
- ARN: `arn:aws:iam::aws:policy/EC2InstanceProfileForImageBuilder`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

EC2InstanceProfileForImageBuilderECRContainerBuilds

Deskripsi: Profil EC2 instance untuk membangun gambar kontainer dengan EC2 Image Builder. Kebijakan ini memberi pengguna izin luas untuk mengunggah gambar ECR.

`EC2InstanceProfileForImageBuilderECRContainerBuilds`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `EC2InstanceProfileForImageBuilderECRContainerBuilds` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 11 Desember 2020, 19:48 UTC
- Waktu yang telah diedit: 11 Desember 2020, 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/EC2InstanceProfileForImageBuilderECRContainerBuilds`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "imagebuilder:GetComponent",
        "imagebuilder:GetContainerRecipe",
        "ecr:GetAuthorizationToken",
        "ecr:BatchGetImage",
        "ecr:InitiateLayerUpload",
        "ecr:UploadLayerPart",
        "ecr:CompleteLayerUpload",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:PutImage"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:imagebuilder:arn",
          "aws:CalledVia" : [
            "imagebuilder.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::ec2imagebuilder*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/imagebuilder/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

ECRReplicationServiceRolePolicy

Deskripsi: Memungkinkan akses ke Layanan AWS dan Sumber Daya yang digunakan atau dikelola oleh Replikasi ECR

`ECRReplicationServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 04 Desember 2020, 22:11 UTC
- Waktu yang telah diedit: 04 Desember 2020, 22:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ECRReplicationServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
        "ecr:CreateRepository",
        "ecr:ReplicateImage"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

ECRTemplateServiceRolePolicy

Deskripsi: Memungkinkan tindakan yang akan dilakukan saat menggunakan templat pembuatan repositori AWS ECR

`ECRTemplateServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 19 Juni 2024, 23:11 UTC
- Waktu yang telah diedit: 19 Juni 2024, 23:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ECRTemplateServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

ElastiCacheServiceRolePolicy

Deskripsi: Kebijakan ini memungkinkan ElastiCache untuk mengelola AWS sumber daya atas nama Anda sebagaimana diperlukan untuk mengelola cache

`ElastiCacheServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 07 Desember 2017, 17:50 UTC
- Waktu telah diedit: 28 November 2023, 03:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ElastiCacheServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ElastiCacheManagementActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:RevokeSecurityGroupIngress",
        "cloudwatch:PutMetricData",
        "outposts:GetOutpost",
```

```
        "outposts:GetOutpostInstanceTypes",
        "outposts:ListOutposts",
        "outposts:ListSites"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateDeleteVPCEndpoints",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringLike" : {
          "ec2:VpceServiceName" : "com.amazonaws.elasticache.serverless.*"
        }
      }
    },
    {
      "Sid" : "TagVPCEndpointsOnCreation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint",
          "aws:RequestTag/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/*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

ElasticLoadBalancingFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon ElasticLoadBalancing, dan akses terbatas ke layanan lain yang diperlukan untuk menyediakan ElasticLoadBalancing fitur.

`ElasticLoadBalancingFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ElasticLoadBalancingFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 20 September 2018, 20:42 UTC
- Waktu telah diedit: 24 Oktober 2024, 22:21 UTC
- ARN: `arn:aws:iam::aws:policy/ElasticLoadBalancingFullAccess`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeRouteTables",
        "ec2:DescribeCoipPools",
        "ec2:GetCoipPoolUsage",
        "ec2: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" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

ElasticLoadBalancingReadOnly

Deskripsi: Menyediakan akses baca saja ke Amazon ElasticLoadBalancing dan layanan dependen

`ElasticLoadBalancingReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ElasticLoadBalancingReadOnly` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 20 September 2018, 20:17 UTC
- Waktu telah diedit: 26 November 2023, 18:15 UTC
- ARN: `arn:aws:iam::aws:policy/ElasticLoadBalancingReadOnly`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Statement1",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:Describe*",
        "elasticloadbalancing:Get*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Statement2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "Statement3",
      "Effect" : "Allow",
      "Action" : "arc-zonal-shift:GetManagedResource",
      "Resource" : "arn:aws:elasticloadbalancing:*:*:loadbalancer/*"
    },
    {
      "Sid" : "Statement4",
      "Effect" : "Allow",
      "Action" : [
        "arc-zonal-shift:ListManagedResources",
        "arc-zonal-shift:ListZonalShifts"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

ElementalActivationsDownloadSoftwareAccess

Deskripsi: Akses untuk melihat aset yang dibeli dan mengunduh perangkat lunak terkait dan file kickstart

`ElementalActivationsDownloadSoftwareAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ElementalActivationsDownloadSoftwareAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 08 September 2020, 17:26 UTC
- Waktu yang telah diedit: September 08, 2020, 17:26 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsDownloadSoftwareAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

ElementalActivationsFullAccess

Deskripsi: Akses penuh untuk melihat dan mengambil tindakan pada aset yang dibeli Elemental Appliances dan Software

`ElementalActivationsFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ElementalActivationsFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 04 Juni 2020, 21:00 UTC
- Waktu yang telah diedit: 04 Juni 2020, 21:00 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

ElementalActivationsGenerateLicenses

Deskripsi: Akses untuk melihat aset yang dibeli dan menghasilkan lisensi perangkat lunak untuk aktivasi yang tertunda

`ElementalActivationsGenerateLicenses`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ElementalActivationsGenerateLicenses` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 Agustus 2020, 18:28 UTC
- Waktu yang telah diedit: 28 Agustus 2020, 18:28 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsGenerateLicenses`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-activations:Get*",
        "elemental-activations:GenerateLicenses",
        "elemental-activations:StartFileUpload",
        "elemental-activations:CompleteFileUpload"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

ElementalActivationsReadOnlyAccess

Deskripsi: Akses hanya-baca ke daftar terperinci aset yang dibeli yang terkait dengan Akun AWS pengguna

`ElementalActivationsReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ElementalActivationsReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 Agustus 2020, 16:51 UTC
- Waktu yang telah diedit: 28 Agustus 2020, 16:51 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

ElementalAppliancesSoftwareFullAccess

Deskripsi: Akses penuh untuk melihat dan mengambil tindakan pada penawaran dan pesanan Elemental Appliances and Software

`ElementalAppliancesSoftwareFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ElementalAppliancesSoftwareFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 31 Juli 2019, 16:28 UTC
- Waktu yang telah diedit: 05 Februari 2021, 21:01 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalAppliancesSoftwareFullAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-appliances-software:*",
        "elemental-activations:CompleteAccountRegistration"
```

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

ElementalAppliancesSoftwareReadOnlyAccess

Deskripsi: Akses hanya-baca untuk melihat penawaran dan pesanan Elemental Appliances and Software

`ElementalAppliancesSoftwareReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ElementalAppliancesSoftwareReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 April 2020, 22:31 UTC
- Waktu yang telah diedit: 01 April 2020, 22:31 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalAppliancesSoftwareReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

ElementalSupportCenterFullAccess

Deskripsi: Akses penuh untuk melihat dan mengambil tindakan pada kasus dukungan Elemental Appliance and Software dan konten dukungan produk

`ElementalSupportCenterFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ElementalSupportCenterFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 25 November 2020, 18:08 UTC
- Waktu yang telah diedit: 05 Februari 2021, 21:02 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalSupportCenterFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-support-cases:*",
        "elemental-support-content:*",
        "elemental-activations:CompleteAccountRegistration"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai kebijakan AWS terkelola dan beralih ke izin dengan hak istimewa paling sedikit

EMRDescribeClusterPolicyForEMRWAL

Deskripsi: Kebijakan ini memberikan izin hanya-baca yang memungkinkan layanan WAL untuk Amazon EMR menemukan dan mengembalikan status klaster

`EMRDescribeClusterPolicyForEMRWAL`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 15 Juni 2023, 23:30 UTC
- Waktu telah diedit: 15 Juni 2023, 23:30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/EMRDescribeClusterPolicyForEMRWAL`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:DescribeCluster"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

FMSServiceRolePolicy

Deskripsi: Kebijakan akses untuk mengizinkan peran tertaut layanan FM melakukan tindakan terkait FM pada sumber daya yang dikelola FM dalam akun Organisasi pelanggan. AWS

`FMSServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 28 Maret 2018, 23:01 UTC
- Waktu yang telah diedit: 21 Mei 2025, 18:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/FMSServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v32 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

FSxDeleteServiceLinkedRoleAccess

Deskripsi: Memungkinkan Amazon FSx menghapus Peran Tertaut Layanan untuk akses Amazon S3

`FSxDeleteServiceLinkedRoleAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan

- Waktu pembuatan: 28 November 2018, 10:40 UTC
- Waktu telah diedit: 28 November 2018, 10:40 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/FSxDeleteServiceLinkedRoleAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus",
        "iam:GetRole"
      ],
      "Resource" : "arn:*:iam::*:role/aws-service-role/s3.data-
source.lustre.fsx.amazonaws.com/AWSServiceRoleForFSxS3Access_*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

GameLiftContainerFleetPolicy

Deskripsi: Memberikan izin yang diperlukan untuk tindakan komputasi dalam armada GameLift penampung Amazon, termasuk akses ke dependensi seperti Amazon S3.

`GameLiftContainerFleetPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `GameLiftContainerFleetPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 12 November 2024, 19:28 UTC
- Waktu telah diedit: 05 Februari 2025, 20:37 UTC
- ARN: `arn:aws:iam::aws:policy/GameLiftContainerFleetPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

GameLiftGameServerGroupPolicy

Deskripsi: Kebijakan untuk mengizinkan Gamelift mengelola sumber GameServerGroups daya pelanggan

`GameLiftGameServerGroupPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `GameLiftGameServerGroupPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 April 2020, 23:12 UTC
- Waktu yang telah diedit: 13 Mei 2020, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/GameLiftGameServerGroupPolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "ec2:TerminateInstances",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/GameLift" : "GameServerGroups"
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:CompleteLifecycleAction",
        "autoscaling:ResumeProcesses",
        "autoscaling:EnterStandby",
        "autoscaling:SetInstanceProtection",
        "autoscaling:UpdateAutoScalingGroup",
        "autoscaling:SuspendProcesses",
        "autoscaling:DetachInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/GameLift" : "GameServerGroups"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "autoscaling:DescribeAutoScalingGroups",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "sns:Publish",
      "Resource" : [
        "arn:*:sns:*:*:ActivatingLifecycleHookTopic-*",
        "arn:*:sns:*:*:TerminatingLifecycleHookTopic-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/GameLift"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

GitLabDuoWithAmazonQPermissionsPolicy

Deskripsi: Kebijakan terkelola ini memberikan izin untuk terhubung dengan Amazon Q dan memanfaatkan fitur di GitLab Duo dengan integrasi Amazon Q.

`GitLabDuoWithAmazonQPermissionsPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `GitLabDuoWithAmazonQPermissionsPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 16 April 2025, 16:37 UTC
- Waktu telah diedit: April 16, 2025, 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/GitLabDuoWithAmazonQPermissionsPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

GlobalAcceleratorFullAccess

Deskripsi: Izinkan GlobalAccelerator Pengguna Akses penuh ke semua APIs

`GlobalAcceleratorFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `GlobalAcceleratorFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 November 2018, 02:44 UTC
- Waktu yang telah diedit: 04 Desember 2020, 19:17 UTC
- ARN: `arn:aws:iam::aws:policy/GlobalAcceleratorFullAccess`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "globalaccelerator:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : "elasticloadbalancing:DescribeLoadBalancers",
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "ec2:DescribeAddresses",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeRegions",
        "ec2:DescribeSubnets"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
globalaccelerator.amazonaws.com/AWSServiceRoleForGlobalAccelerator*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "globalaccelerator.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

GlobalAcceleratorReadOnlyAccess

Deskripsi: Izinkan GlobalAccelerator Pengguna Akses untuk Hanya Membaca APIs

`GlobalAcceleratorReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `GlobalAcceleratorReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 November 2018, 02:41 UTC
- Waktu telah diedit: 27 November 2018, 02:41 UTC
- ARN: `arn:aws:iam::aws:policy/GlobalAcceleratorReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
  "Statement" : [
    {
      "Action" : [
        "globalaccelerator:Describe*",
        "globalaccelerator:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

GreengrassOTAUpdateArtifactAccess

Deskripsi: Menyediakan akses baca ke artefak Pembaruan Greengrass OTA di semua wilayah Greengrass

`GreengrassOTAUpdateArtifactAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `GreengrassOTAUpdateArtifactAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 29 November 2017, 18:11 UTC
- Waktu telah diedit: 18 Desember 2018, 00:59 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/GreengrassOTAUpdateArtifactAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowsIotToAccessGreengrassOTAUpdateArtifacts",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*-greengrass-updates/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

GroundTruthSyntheticConsoleFullAccess

Deskripsi: Kebijakan ini memberikan izin yang diperlukan untuk menggunakan semua fitur SageMaker Ground Truth Synthetic Console.

`GroundTruthSyntheticConsoleFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `GroundTruthSyntheticConsoleFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 25 Agustus 2022, 15:58 UTC
- Waktu yang telah diedit: 25 Agustus 2022, 15.58 UTC
- ARN: `arn:aws:iam::aws:policy/GroundTruthSyntheticConsoleFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker-groundtruth-synthetic:*",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

GroundTruthSyntheticConsoleReadOnlyAccess

Deskripsi: Kebijakan ini memberikan akses hanya-baca ke SageMaker Ground Truth Synthetic melalui. AWS Management Console

`GroundTruthSyntheticConsoleReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `GroundTruthSyntheticConsoleReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 25 Agustus 2022, 15:58 UTC
- Waktu yang telah diedit: 25 Agustus 2022, 15.58 UTC
- ARN: `arn:aws:iam::aws:policy/GroundTruthSyntheticConsoleReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      "Effect" : "Allow",
      "Action" : [
        "sagemaker-groundtruth-synthetic:List*",
        "sagemaker-groundtruth-synthetic:Get*",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

Health_OrganizationsServiceRolePolicy

Deskripsi: Kebijakan AWS Kesehatan untuk mengaktifkan fitur Tampilan Organisasi

`Health_OrganizationsServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 16 Desember 2019, 13:28 UTC
- Waktu telah diedit: 06 Februari 2024, 16:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Health_OrganizationsServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "HealthAPIOrganizationView0",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

IAMAccessAdvisorReadOnly

Deskripsi: Kebijakan ini memberikan akses untuk membaca semua informasi akses yang disediakan oleh penasihat akses IAM seperti informasi layanan yang terakhir diakses.

`IAMAccessAdvisorReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `IAMAccessAdvisorReadOnly` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 21 Juni 2019, 19:33 UTC
- Waktu yang telah diedit: 21 Juni 2019, 19:33 UTC
- ARN: `arn:aws:iam::aws:policy/IAMAccessAdvisorReadOnly`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "iam:ListUsers",
        "iam:ListGroups",
        "iam:ListPolicies",
        "iam:ListPoliciesGrantingServiceAccess",
        "iam:GenerateServiceLastAccessedDetails",
        "iam:GenerateOrganizationsAccessReport",
        "iam:GenerateCredentialReport",
        "iam:GetRole",
        "iam:GetPolicy",
        "iam:GetServiceLastAccessedDetails",
        "iam:GetServiceLastAccessedDetailsWithEntities",
        "iam:GetOrganizationsAccessReport",
```

```
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribePolicy",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:ListPoliciesForTarget",
        "organizations:ListRoots",
        "organizations:ListPolicies",
        "organizations:ListTargetsForPolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

IAMAccessAnalyzerFullAccess

Deskripsi: Menyediakan akses penuh ke IAM Access Analyzer

`IAMAccessAnalyzerFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `IAMAccessAnalyzerFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 02 Desember 2019, 17:12 UTC
- Waktu yang telah diedit: 02 Desember 2019, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/IAMAccessAnalyzerFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "access-analyzer.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListChildren",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
```

```
        "organizations:ListRoots"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

IAMAccessAnalyzerReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke sumber daya IAM Access Analyzer

`IAMAccessAnalyzerReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `IAMAccessAnalyzerReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 02 Desember 2019, 17:12 UTC
- Waktu yang telah diedit: 18 Juli 2024, 17:49 UTC
- ARN: `arn:aws:iam::aws:policy/IAMAccessAnalyzerReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

IAMFullAccess

Deskripsi: Menyediakan akses penuh ke IAM melalui. AWS Management Console

`IAMFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `IAMFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu yang telah diedit: 21 Juni 2019, 19:40 UTC
- ARN: `arn:aws:iam::aws:policy/IAMFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:*",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribePolicy",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:ListPoliciesForTarget",
        "organizations:ListRoots",
        "organizations:ListPolicies",
        "organizations:ListTargetsForPolicy"
      ],
```

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

IAMReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke IAM melalui. AWS Management Console

`IAMReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `IAMReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu telah diedit: 25 Januari 2018, 19:11 UTC
- ARN: `arn:aws:iam::aws:policy/IAMReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GenerateCredentialReport",
        "iam:GenerateServiceLastAccessedDetails",
        "iam:Get*",
        "iam:List*",
        "iam:SimulateCustomPolicy",
        "iam:SimulatePrincipalPolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

IAMSelfManageServiceSpecificCredentials

Deskripsi: Memungkinkan pengguna IAM untuk mengelola Kredenal Khusus Layanan mereka sendiri.

`IAMSelfManageServiceSpecificCredentials`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `IAMSelfManageServiceSpecificCredentials` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 22 Desember 2016, 17:25 UTC
- Waktu telah diedit: 22 Desember 2016, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/IAMSelfManageServiceSpecificCredentials`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceSpecificCredential",
        "iam:ListServiceSpecificCredentials",
        "iam:UpdateServiceSpecificCredential",
        "iam:DeleteServiceSpecificCredential",
        "iam:ResetServiceSpecificCredential"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

IAMUserChangePassword

Deskripsi: Memberikan kemampuan bagi pengguna IAM untuk mengubah kata sandi mereka sendiri.

`IAMUserChangePassword`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `IAMUserChangePassword` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 15 November 2016, 00:25 UTC
- Waktu yang telah diedit: 29 Mei 2025, 21:52 UTC
- ARN: `arn:aws:iam::aws:policy/IAMUserChangePassword`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

IAMUserSSHKeys

Deskripsi: Memberikan kemampuan bagi pengguna IAM untuk mengelola kunci SSH mereka sendiri.

`IAMUserSSHKeys`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `IAMUserSSHKeys` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 09 Juli 2015, 17:08 UTC
- Waktu telah diedit: 09 Juli 2015, 17:08 UTC
- ARN: `arn:aws:iam::aws:policy/IAMUserSSHKeys`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteSSHPublicKey",
        "iam:GetSSHPublicKey",
        "iam:ListSSHPublicKeys",
        "iam:UpdateSSHPublicKey",
        "iam:UploadSSHPublicKey"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

IVSFullAccess

Deskripsi: Menyediakan akses penuh ke Layanan Video Interaktif (IVS), Juga termasuk izin untuk layanan dependen, diperlukan untuk akses penuh ke konsol ivs.

`IVSFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `IVSFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 13 Desember 2023, 21:20 UTC
- Waktu telah diedit: 13 Desember 2023, 21:20 UTC
- ARN: `arn:aws:iam::aws:policy/IVSFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

IVSReadOnlyAccess

Deskripsi: Menyediakan akses hanya-baca ke streaming IVS Low-Latency dan Real-Time APIs

`IVSReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `IVSReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 05 Desember 2023, 18:00 UTC
- Waktu telah diedit: 17 September 2024, 20:42 UTC
- ARN: `arn:aws:iam::aws:policy/IVSReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "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:ListParticipantEvents",
        "ivs:ListPlaybackKeyPairs",
        "ivs:ListPlaybackRestrictionPolicies",
        "ivs:ListPublicKeys",
        "ivs:ListRecordingConfigurations",
        "ivs:ListStages",
        "ivs:ListStageSessions",
        "ivs:ListStorageConfigurations",
        "ivs:ListStreamKeys",
        "ivs:ListStreams",
        "ivs:ListStreamSessions",
        "ivs:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

IVSRecordToS3

Deskripsi: Peran Tertaut Layanan untuk melakukan S3 PutObject untuk merekam streaming langsung IVS

`IVSRecordToS3`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 05 Desember 2020, 00:10 UTC
- Waktu yang telah diedit: 05 Desember 2020, 00:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/IVSRecordToS3`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::AWSIVS_*/ivs/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

KafkaConnectServiceRolePolicy

Deskripsi: Kebijakan ini memberikan izin kepada Kafka Connect untuk mengelola AWS sumber daya atas nama Anda.

`KafkaConnectServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 07 September 2021, 13:12 UTC

- Waktu yang telah diedit: 07 September 2021, 13:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/KafkaConnectServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

KafkaServiceRolePolicy

Deskripsi: Kebijakan peran terkait layanan IAM untuk Kafka.

`KafkaServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 15 November 2018, 23:31 UTC
- Waktu yang telah diedit: 28 April 2023, 00:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/KafkaServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:AttachNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DetachNetworkInterface",
        "ec2:DescribeVpcEndpoints",
        "acm-pca:GetCertificateAuthorityCertificate",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource" : "arn:*:ec2:*:*:subnet/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVpcEndpoints",
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource" : "arn:*:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AWSMSKManaged" : "true"
        },
        "StringLike" : {
          "ec2:ResourceTag/ClusterArn" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:PutResourcePolicy",
        "secretsmanager:DeleteResourcePolicy",
        "secretsmanager:DescribeSecret"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "secretsmanager:SecretId" : "arn:*:secretsmanager:*:*:secret:AmazonMSK_*"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

KeyspacesCDCServiceRolePolicy

Deskripsi: Memberikan izin yang diperlukan ke Amazon Keyspaces untuk Mengubah Pengambilan Data

`KeyspacesCDCServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 21 Juni 2025, 00:22 UTC
- Waktu yang telah diedit: 21 Juni 2025, 00:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/KeyspacesCDCServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

KeyspacesReplicationServiceRolePolicy

Deskripsi: Izin yang diperlukan oleh Keyspaces untuk replikasi data lintas wilayah

`KeyspacesReplicationServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 02 Mei 2023, 16:15 UTC

- Waktu telah diedit: 15 November 2024, 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/KeyspacesReplicationServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

LakeFormationDataAccessServiceRolePolicy

Deskripsi: Kebijakan untuk memberikan akses data sementara ke sumber daya Lake Formation

`LakeFormationDataAccessServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 20 Juni 2019, 20:46 UTC
- Waktu telah diedit: 06 Februari 2024, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LakeFormationDataAccessServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LakeFormationDataAccessServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

LexBotPolicy

Deskripsi: Kebijakan untuk kasus penggunaan AWS Lex Bot

`LexBotPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 17 Februari 2017, 22:18 UTC
- Waktu yang telah diedit: 13 November 2019, 22:29 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LexBotPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      "Effect" : "Allow",
      "Action" : [
        "polly:SynthesizeSpeech"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "comprehend:DetectSentiment"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

LexChannelPolicy

Deskripsi: Kebijakan untuk kasus penggunaan AWS Lex Channel

`LexChannelPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan

- Waktu pembuatan: 17 Februari 2017, 23:23 UTC
- Waktu telah diedit: 17 Februari 2017, 23:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LexChannelPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

LightsailExportAccess

Deskripsi: AWS Kebijakan peran terkait layanan Lightsail yang memberikan izin untuk mengekspor sumber daya

`LightsailExportAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 28 September 2018, 16:35 UTC
- Waktu telah diedit: 15 Januari 2022, 01:45 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LightsailExportAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/lightsail.amazonaws.com/
AWSServiceRoleForLightsail*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopySnapshot",
```

```
        "ec2:DescribeSnapshots",
        "ec2:CopyImage",
        "ec2:DescribeImages"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetAccountPublicAccessBlock"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

MediaConnectGatewayInstanceRolePolicy

Deskripsi: Kebijakan ini memberikan izin untuk mendaftarkan Instans MediaConnect Gateway ke Gateway. MediaConnect

`MediaConnectGatewayInstanceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `MediaConnectGatewayInstanceRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 22 Maret 2023, 20:43 UTC
- Waktu telah diedit: 22 Maret 2023, 20:43 UTC
- ARN: `arn:aws:iam::aws:policy/MediaConnectGatewayInstanceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MediaConnectGateway",
      "Effect" : "Allow",
      "Action" : [
        "mediaconnect:DiscoverGatewayPollEndpoint",
        "mediaconnect:PollGateway",
        "mediaconnect:SubmitGatewayStateChange"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

MediaPackageServiceRolePolicy

Deskripsi: Memungkinkan MediaPackage untuk mempublikasikan log ke CloudWatch

`MediaPackageServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 18 September 2020, 17:45 UTC
- Waktu yang telah diedit: 18 September 2020, 17:45 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MediaPackageServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "logs:PutLogEvents",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/MediaPackage/*:log-stream:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams"
```

```
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/MediaPackage/*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

MemoryDBServiceRolePolicy

Deskripsi: Kebijakan ini memungkinkan MemoryDB mengelola AWS sumber daya atas nama Anda sebagaimana diperlukan untuk mengelola sumber daya Anda.

`MemoryDBServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 17 Agustus 2021 22:34 UTC
- Waktu telah diedit: 01 Desember 2024, 16:21 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MemoryDBServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

MigrationHubDMSAccessServiceRolePolicy

Deskripsi: Kebijakan Layanan Migrasi Database untuk berperan dalam akun pelanggan untuk memanggil Migration Hub

`MigrationHubDMSAccessServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 12 Juni 2019, 17:50 UTC
- Waktu yang telah diedit: 07 Oktober 2019, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MigrationHubDMSAccessServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "mgh:CreateProgressUpdateStream",
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/DMS"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:DescribeMigrationTask",
        "mgh:AssociateDiscoveredResource",
        "mgh:ListDiscoveredResources",
        "mgh:ImportMigrationTask",
        "mgh:ListCreatedArtifacts",
        "mgh:DisassociateDiscoveredResource",
        "mgh:AssociateCreatedArtifact",
        "mgh:NotifyMigrationTaskState",
        "mgh:DisassociateCreatedArtifact",
        "mgh:PutResourceAttributes"
      ],
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/DMS/migrationTask/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:ListMigrationTasks",
        "mgh:NotifyApplicationState",
        "mgh:DescribeApplicationState",
        "mgh:GetHomeRegion"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

MigrationHubServiceRolePolicy

Deskripsi: Memungkinkan Migration Hub memanggil Application Discovery Service atas nama Anda

`MigrationHubServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 12 Juni 2019, 17:22 UTC
- Waktu yang telah diedit: 06 Agustus 2020, 18:08 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MigrationHubServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
    {
      "Effect" : "Allow",
      "Action" : [
        "discovery:ListConfigurations",
        "discovery:DescribeConfigurations"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "aws:migrationhub:source-id"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "dms:AddTagsToResource",
      "Resource" : [
        "arn:aws:dms:*:*:endpoint:*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "aws:migrationhub:source-id"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceAttribute"
      ],
      "Resource" : [
        "*"
      ]
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

MigrationHubSMSAccessServiceRolePolicy

Deskripsi: Kebijakan Layanan Migrasi Server untuk berperan dalam akun pelanggan untuk memanggil Migration Hub

`MigrationHubSMSAccessServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 12 Juni 2019, 18:30 UTC
- Waktu yang telah diedit: 07 Oktober 2019, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MigrationHubSMSAccessServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "mgh:CreateProgressUpdateStream",
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/SMS"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:DescribeMigrationTask",
        "mgh:AssociateDiscoveredResource",
        "mgh:ListDiscoveredResources",
        "mgh:ImportMigrationTask",
        "mgh:ListCreatedArtifacts",
        "mgh:DisassociateDiscoveredResource",
        "mgh:AssociateCreatedArtifact",
        "mgh:NotifyMigrationTaskState",
        "mgh:DisassociateCreatedArtifact",
        "mgh:PutResourceAttributes"
      ],
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/SMS/migrationTask/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:ListMigrationTasks",
        "mgh:NotifyApplicationState",
        "mgh:DescribeApplicationState",
        "mgh:GetHomeRegion"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM

- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

MonitronServiceRolePolicy

Deskripsi: Kebijakan untuk peran terkait layanan AWS Monitron yang memberikan akses ke sumber daya pelanggan yang diperlukan.

`MonitronServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 02 Mei 2022, 19:22 UTC
- Waktu yang telah diedit: 02 Mei 2022 19.22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MonitronServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/monitron/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

MultiPartyApprovalFullAccess

Deskripsi: Menyediakan akses penuh ke persetujuan Multi-pihak. Kebijakan ini juga mencakup izin terkait untuk AWS Organizations dan AWS IAM Identity untuk mengelola tim persetujuan dan sumber identitas.

`MultiPartyApprovalFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `MultiPartyApprovalFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 Juni 2025, 20:22 UTC
- Waktu telah diedit: 18 Juni 2025, 20:22 UTC
- ARN: `arn:aws:iam::aws:policy/MultiPartyApprovalFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

MultiPartyApprovalReadOnlyAccess

Deskripsi: Menyediakan akses hanya-baca ke persetujuan Multi-pihak. Kebijakan ini juga mencakup izin baca terkait dengan AWS Organizations dan AWS IAM Identity untuk tim persetujuan dan sumber identitas.

`MultiPartyApprovalReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `MultiPartyApprovalReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 Juni 2025, 20:07 UTC
- Waktu yang telah diedit: 18 Juni 2025, 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/MultiPartyApprovalReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

NeptuneConsoleFullAccess

Deskripsi: Menyediakan akses penuh untuk mengelola Amazon Neptunus menggunakan file. AWS Management Console Perhatikan kebijakan ini juga memberikan akses penuh untuk mempublikasikan semua topik SNS dalam akun, izin untuk membuat dan mengedit EC2 instans Amazon dan konfigurasi VPC, izin untuk melihat dan mencantumkan kunci di Amazon KMS, dan akses penuh ke Amazon RDS. Untuk informasi lebih lanjut, lihat https://aws.amazon.com/neptune/faqs/.

`NeptuneConsoleFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `NeptuneConsoleFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 19 Juni 2018, 21:35 UTC
- Waktu telah diedit: November 30, 2023, 07:32 UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneConsoleFullAccess`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowNeptuneCreate",
      "Effect" : "Allow",
      "Action" : [
        "rds:CreateDBCluster",
        "rds:CreateDBInstance"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "rds:DatabaseEngine" : [
            "graphdb",
            "neptune"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "AllowManagementPermissionsForRDS",
      "Action" : [
        "rds:AddRoleToDBCluster",
        "rds:AddSourceIdentifierToSubscription",
        "rds:AddTagsToResource",
        "rds:ApplyPendingMaintenanceAction",
        "rds:CopyDBClusterParameterGroup",
        "rds:CopyDBClusterSnapshot",
        "rds:CopyDBParameterGroup",
        "rds:CreateDBClusterParameterGroup",
        "rds:CreateDBClusterSnapshot",
        "rds:CreateDBParameterGroup",
        "rds:CreateDBSubnetGroup",
        "rds:CreateEventSubscription",
        "rds:DeleteDBCluster",
        "rds:DeleteDBClusterParameterGroup",
        "rds:DeleteDBClusterSnapshot",
        "rds:DeleteDBInstance",
        "rds:DeleteDBParameterGroup",
        "rds:DeleteDBSubnetGroup",
        "rds:DeleteEventSubscription",
        "rds:DescribeAccountAttributes",
        "rds:DescribeCertificates",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBLogFiles",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultClusterParameters",
        "rds:DescribeEngineDefaultParameters",
        "rds:DescribeEventCategories",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeEvents",
```

```
        "rds:DescribeOptionGroups",
        "rds:DescribeOrderableDBInstanceOptions",
        "rds:DescribePendingMaintenanceActions",
        "rds:DescribeValidDBInstanceModifications",
        "rds:DownloadDBLogFilePortion",
        "rds:FailoverDBCluster",
        "rds:ListTagsForResource",
        "rds:ModifyDBCluster",
        "rds:ModifyDBClusterParameterGroup",
        "rds:ModifyDBClusterSnapshotAttribute",
        "rds:ModifyDBInstance",
        "rds:ModifyDBParameterGroup",
        "rds:ModifyDBSubnetGroup",
        "rds:ModifyEventSubscription",
        "rds:PromoteReadReplicaDBCluster",
        "rds:RebootDBInstance",
        "rds:RemoveRoleFromDBCluster",
        "rds:RemoveSourceIdentifierFromSubscription",
        "rds:RemoveTagsFromResource",
        "rds:ResetDBClusterParameterGroup",
        "rds:ResetDBParameterGroup",
        "rds:RestoreDBClusterFromSnapshot",
        "rds:RestoreDBClusterToPointInTime"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "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"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

NeptuneFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Neptunus. Perhatikan kebijakan ini juga memberikan akses penuh untuk mempublikasikan semua topik SNS dalam akun dan akses penuh ke Amazon RDS. Untuk informasi lebih lanjut, lihat https://aws.amazon.com/neptune/ faqs/.

`NeptuneFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `NeptuneFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 Mei 2018, 19:17 UTC
- Waktu telah diedit: 22 Januari 2024, 16:32 UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneFullAccess`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowNeptuneCreate",
      "Effect" : "Allow",
      "Action" : [
        "rds:CreateDBCluster",
        "rds:CreateDBInstance"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "rds:DatabaseEngine" : [
            "graphdb",
            "neptune"
          ]
        }
      }
    },
    {
      "Sid" : "AllowManagementPermissionsForRDS",
      "Effect" : "Allow",
      "Action" : [
        "rds:AddRoleToDBCluster",
        "rds:AddSourceIdentifierToSubscription",
        "rds:AddTagsToResource",
        "rds:ApplyPendingMaintenanceAction",
        "rds:CopyDBClusterParameterGroup",
        "rds:CopyDBClusterSnapshot",
        "rds:CopyDBParameterGroup",
        "rds:CreateDBClusterEndpoint",
        "rds:CreateDBClusterParameterGroup",
        "rds:CreateDBClusterSnapshot",
        "rds:CreateDBParameterGroup",
        "rds:CreateDBSubnetGroup",
        "rds:CreateEventSubscription",
        "rds:CreateGlobalCluster",
        "rds:DeleteDBCluster",
        "rds:DeleteDBClusterEndpoint",
        "rds:DeleteDBClusterParameterGroup",
        "rds:DeleteDBClusterSnapshot",
        "rds:DeleteDBInstance",
```

```
        "rds:DeleteDBParameterGroup",
        "rds:DeleteDBSubnetGroup",
        "rds:DeleteEventSubscription",
        "rds:DeleteGlobalCluster",
        "rds:DescribeDBClusterEndpoints",
        "rds:DescribeAccountAttributes",
        "rds:DescribeCertificates",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBLogFiles",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultClusterParameters",
        "rds:DescribeEngineDefaultParameters",
        "rds:DescribeEventCategories",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeEvents",
        "rds:DescribeGlobalClusters",
        "rds:DescribeOptionGroups",
        "rds:DescribeOrderableDBInstanceOptions",
        "rds:DescribePendingMaintenanceActions",
        "rds:DescribeValidDBInstanceModifications",
        "rds:DownloadDBLogFilePortion",
        "rds:FailoverDBCluster",
        "rds:FailoverGlobalCluster",
        "rds:ListTagsForResource",
        "rds:ModifyDBCluster",
        "rds:ModifyDBClusterEndpoint",
        "rds:ModifyDBClusterParameterGroup",
        "rds:ModifyDBClusterSnapshotAttribute",
        "rds:ModifyDBInstance",
        "rds:ModifyDBParameterGroup",
        "rds:ModifyDBSubnetGroup",
        "rds:ModifyEventSubscription",
        "rds:ModifyGlobalCluster",
        "rds:PromoteReadReplicaDBCluster",
        "rds:RebootDBInstance",
```

```
        "rds:RemoveFromGlobalCluster",
        "rds:RemoveRoleFromDBCluster",
        "rds:RemoveSourceIdentifierFromSubscription",
        "rds: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" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

NeptuneGraphReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke semua sumber daya Amazon Neptunus Analytics bersama dengan izin baca saja untuk layanan dependen.

`NeptuneGraphReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `NeptuneGraphReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 November 2023, 07:32 UTC
- Waktu telah diedit: November 30, 2023, 07:32 UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneGraphReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadOnlyPermissionsForNeptuneGraph",
      "Effect" : "Allow",
      "Action" : [
        "neptune-graph:Get*",
        "neptune-graph:List*",
        "neptune-graph:Read*"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "AllowReadOnlyPermissionsForEC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadOnlyPermissionsForKMS",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadOnlyPermissionsForCloudwatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadOnlyPermissionsForLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:GetLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/neptune/*:log-stream:*"
      ]
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

NeptuneReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon Neptunus. Perhatikan bahwa kebijakan ini juga memberikan akses ke sumber daya Amazon RDS. Untuk informasi lebih lanjut, lihat https:// aws.amazon.com/neptune/ faqs/.

`NeptuneReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `NeptuneReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 Mei 2018, 19:16 UTC
- Waktu telah diedit: 22 Januari 2024, 16:33 UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadOnlyPermissionsForRDS",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeAccountAttributes",
        "rds:DescribeCertificates",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBLogFiles",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEventCategories",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeEvents",
        "rds:DescribeGlobalClusters",
        "rds:DescribeOrderableDBInstanceOptions",
        "rds:DescribePendingMaintenanceActions",
        "rds:DownloadDBLogFilePortion",
        "rds:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadOnlyPermissionsForCloudwatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "AllowReadOnlyPermissionsForEC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadOnlyPermissionsForKMS",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
        "kms:ListRetirableGrants",
        "kms:ListAliases",
        "kms:ListKeyPolicies"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadOnlyPermissionsForLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:GetLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/rds/*:log-stream:*",
        "arn:aws:logs:*:*:log-group:/aws/neptune/*:log-stream:*"
      ]
    },
    {
      "Sid" : "AllowReadOnlyPermissionsForNeptuneDB",
      "Effect" : "Allow",
      "Action" : [
        "neptune-db:Read*",
        "neptune-db:Get*",
        "neptune-db:List*"
      ],
```

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

NetworkAdministrator

Deskripsi: Memberikan izin akses penuh ke AWS layanan dan tindakan yang diperlukan untuk menyiapkan dan mengonfigurasi sumber daya AWS jaringan.

`NetworkAdministrator`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `NetworkAdministrator` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan fungsi Job
- Waktu pembuatan: 10 November 2016, 17:31 UTC
- Waktu yang telah diedit: 19 Desember 2024, 22:52 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/NetworkAdministrator`

Versi kebijakan

Versi kebijakan: v13 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

NetworkSecurityDirectorServiceLinkedRolePolicy

Deskripsi: Memberikan izin untuk peran terkait layanan direktur keamanan jaringan AWS Shield untuk menilai lingkungan tertentu.

`NetworkSecurityDirectorServiceLinkedRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 13 Juni 2025, 20:07 UTC
- Waktu yang telah diedit: 13 Juni 2025, 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/NetworkSecurityDirectorServiceLinkedRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

OAMFullAccess

Deskripsi: Menyediakan akses penuh ke CloudWatch Observability Access Manager

`OAMFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `OAMFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 November 2022, 13:38 UTC
- Waktu yang telah diedit: 27 November 2022, 13.38 UTC
- ARN: `arn:aws:iam::aws:policy/OAMFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

OAMReadOnlyAccess

Deskripsi: Menyediakan akses Hanya Baca ke Manajer Akses CloudWatch Observabilitas

`OAMReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `OAMReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 November 2022, 13:29 UTC
- Waktu yang telah diedit: 27 November 2022, 13.29 UTC
- ARN: `arn:aws:iam::aws:policy/OAMReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

OpensearchIngestionSelfManagedVpcePolicy

Deskripsi: Memungkinkan Amazon OpenSearch Ingestion untuk mendeskripsikan sumber daya jaringan dan menulis metrik layanan ke cloudwatch

`OpensearchIngestionSelfManagedVpcePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 10 Juni 2024, 19:59 UTC
- Waktu yang telah diedit: 10 Juni 2024, 19:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/OpensearchIngestionSelfManagedVpcePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

PartnerCentralAccountManagementUserRoleAssociation

Deskripsi: Menyediakan akses untuk mengasosiasikan dan memisahkan pengguna pusat mitra dengan peran IAM

`PartnerCentralAccountManagementUserRoleAssociation`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `PartnerCentralAccountManagementUserRoleAssociation` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 10 November 2023, 02:03 UTC
- Waktu telah diedit: 10 November 2023, 02:03 UTC
- ARN: `arn:aws:iam::aws:policy/PartnerCentralAccountManagementUserRoleAssociation`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PassPartnerCentralRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/PartnerCentralRoleFor*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "partnercentral-account-management.amazonaws.com"
        }
```

```
      }
    },
    {
      "Sid" : "PartnerUserRoleAssociation",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "partnercentral-account-management:AssociatePartnerUser",
        "partnercentral-account-management:DisassociatePartnerUser"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

PowerUserAccess

Deskripsi: Menyediakan akses penuh ke AWS layanan dan sumber daya, tetapi tidak mengizinkan pengelolaan Pengguna dan grup.

`PowerUserAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `PowerUserAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:39 UTC
- Waktu yang telah diedit: 29 April 2025, 19:07 UTC
- ARN: `arn:aws:iam::aws:policy/PowerUserAccess`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

QAppsServiceRolePolicy

Deskripsi: Memberikan izin Layanan AWS dan Sumber Daya yang digunakan atau dikelola oleh Amazon Q Apps.

`QAppsServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 26 September 2024, 19:22 UTC
- Waktu telah diedit: September 26, 2024, 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/QAppsServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
  "Statement" : [
    {
      "Sid" : "QAppsPutMetricDataPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/QApps"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

QBusinessQuicksightPluginPolicy

Deskripsi: Memberikan izin QBusiness QuickSight APIs untuk memanggil plugin QuickSight

`QBusinessQuicksightPluginPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `QBusinessQuicksightPluginPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 Desember 2024, 15:36 UTC
- Waktu telah diedit: 03 Desember 2024, 15:36 UTC
- ARN: `arn:aws:iam::aws:policy/QBusinessQuicksightPluginPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "QBusinessToQuickSightPredictQAResultsInvocation",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:PredictQAResults"
      ],
      "Resource" : [
        "arn:aws:quicksight:*:*:topic/*",
        "arn:aws:quicksight:*:*:dashboard/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

QBusinessServiceRolePolicy

Deskripsi: Memberikan izin Layanan AWS dan Sumber Daya yang digunakan atau dikelola oleh Amazon Q

`QBusinessServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 29 April 2024, 16:05 UTC
- Waktu yang telah diedit: 29 April 2024, 16:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/QBusinessServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "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}"
        }
```

```
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

QuickSightAccessForS3StorageManagementAnalyticsReadOnly

Deskripsi: Kebijakan yang digunakan oleh QuickSight tim untuk mengakses data pelanggan yang dihasilkan oleh S3 Storage Management Analytics.

`QuickSightAccessForS3StorageManagementAnalyticsReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `QuickSightAccessForS3StorageManagementAnalyticsReadOnly` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 12 Juni 2017, 18:18 UTC
- Waktu yang telah diedit: 08 Oktober 2019, 23:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/QuickSightAccessForS3StorageManagementAnalyticsReadOnly`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::s3-analytics-export-shared-*"
      ]
    },
    {
      "Action" : [
        "s3:GetAnalyticsConfiguration",
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

RDSCloudHsmAuthorizationRole

Deskripsi: Kebijakan default untuk peran layanan Amazon RDS.

`RDSCloudHsmAuthorizationRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `RDSCloudHsmAuthorizationRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu yang telah diedit: 26 September 2019, 22:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/RDSCloudHsmAuthorizationRole`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudhsm:CreateLunaClient",
        "cloudhsm:DeleteLunaClient",
        "cloudhsm:DescribeHapg",
        "cloudhsm:DescribeLunaClient",
        "cloudhsm:GetConfig",
        "cloudhsm:ModifyHapg",
        "cloudhsm:ModifyLunaClient"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

ReadOnlyAccess

Deskripsi: Menyediakan akses hanya-baca ke AWS layanan dan sumber daya.

`ReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:39 UTC
- Waktu yang telah diedit: 03 Juni 2025, 19:07 UTC
- ARN: `arn:aws:iam::aws:policy/ReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v129 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "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:GetChallengeQuestions",
        "account:GetContactInformation",
        "account:GetPrimaryEmail",
        "account:GetRegionOptStatus",
        "account:ListRegions",
        "acm-pca:Describe*",
        "acm-pca:Get*",
        "acm-pca:List*",
        "acm:Describe*",
        "acm:Get*",
        "acm:List*",
        "aiops:GetInvestigation",
        "aiops:GetInvestigationEvent",
        "aiops:GetInvestigationGroup",
        "aiops:GetInvestigationResource",
        "aiops:ListInvestigationEvents",
        "aiops:ListInvestigationGroups",
        "aiops:ListInvestigations",
        "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: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",
        "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-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: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: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: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:GetCostAndUsageWithResources",
        "ce:GetCostCategories",
        "ce:GetCostForecast",
        "ce:GetDimensionValues",
        "ce:GetPreferences",
        "ce:GetReservationCoverage",
        "ce:GetReservationPurchaseRecommendation",
        "ce:GetReservationUtilization",
        "ce:GetRightsizingRecommendation",
        "ce:GetSavingsPlanPurchaseRecommendationDetails",
        "ce:GetSavingsPlansCoverage",
        "ce:GetSavingsPlansPurchaseRecommendation",
        "ce:GetSavingsPlansUtilization",
        "ce:GetSavingsPlansUtilizationDetails",
        "ce:GetTags",
        "ce:GetUsageForecast",
        "ce: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",
        "cloud9:Describe*",
        "cloud9:List*",
        "clouddirectory:BatchRead",
        "clouddirectory:Get*",
        "clouddirectory:List*",
        "clouddirectory:LookupPolicy",
        "cloudformation:Describe*",
        "cloudformation:Detect*",
        "cloudformation:Estimate*",
        "cloudformation:Get*",
        "cloudformation:List*",
        "cloudformation:ValidateTemplate",
        "cloudfront-keyvaluestore:Describe*",
        "cloudfront-keyvaluestore:Get*",
        "cloudfront-keyvaluestore:List*",
        "cloudfront:Describe*",
        "cloudfront:Get*",
        "cloudfront:List*",
        "cloudhsm:Describe*",
        "cloudhsm:List*",
        "cloudsearch:Describe*",
        "cloudsearch:List*",
        "cloudtrail:Describe*",
        "cloudtrail:Get*",
        "cloudtrail:List*",
        "cloudtrail:LookupEvents",
        "cloudwatch:Describe*",
        "cloudwatch:GenerateQuery",
```

```
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "codeartifact:DescribeDomain",
        "codeartifact:DescribePackage",
        "codeartifact:DescribePackageVersion",
        "codeartifact:DescribeRepository",
        "codeartifact:GetAuthorizationToken",
        "codeartifact:GetDomainPermissionsPolicy",
        "codeartifact:GetPackageVersionAsset",
        "codeartifact:GetPackageVersionReadme",
        "codeartifact:GetRepositoryEndpoint",
        "codeartifact:GetRepositoryPermissionsPolicy",
        "codeartifact:ListDomains",
        "codeartifact: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*",
        "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:ListCommonControls",
        "controlcatalog:ListDomains",
        "controlcatalog:ListObjectives",
        "cost-optimization-hub:GetPreferences",
        "cost-optimization-hub:GetRecommendation",
        "cost-optimization-hub:ListEnrollmentStatuses",
        "cost-optimization-hub:ListRecommendationSummaries",
        "cost-optimization-hub:ListRecommendations",
        "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*",
        "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: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: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",
        "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:BatchGetFreeTrialInfo",
        "inspector2:DescribeOrganizationConfiguration",
        "inspector2:GetDelegatedAdminAccount",
        "inspector2:GetFindingsReportStatus",
        "inspector2:GetMember",
        "inspector2:ListAccountPermissions",
        "inspector2:ListCisScans",
        "inspector2:ListCoverage",
        "inspector2:ListCoverageStatistics",
        "inspector2:ListDelegatedAdminAccounts",
        "inspector2:ListFilters",
        "inspector2:ListFindingAggregations",
        "inspector2:ListFindings",
        "inspector2:ListMembers",
        "inspector2:ListTagsForResource",
        "inspector2:ListUsageTotals",
        "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",
        "iotroborunner:GetDestination",
        "iotroborunner:GetSite",
        "iotroborunner:GetWorker",
        "iotroborunner:GetWorkerFleet",
        "iotroborunner:ListDestinations",
        "iotroborunner:ListSites",
        "iotroborunner:ListWorkerFleets",
        "iotroborunner:ListWorkers",
        "iotsitewise:Describe*",
        "iotsitewise:Get*",
        "iotsitewise:List*",
        "iotwireless:GetDestination",
        "iotwireless:GetDeviceProfile",
        "iotwireless:GetEventConfigurationByResourceTypes",
        "iotwireless:GetFuotaTask",
        "iotwireless:GetLogLevelsByResourceTypes",
        "iotwireless: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",
        "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:DescribeChannel",
        "medialive:DescribeInput",
```

```
        "medialive:DescribeInputDevice",
        "medialive:DescribeInputDeviceThumbnail",
        "medialive:DescribeInputSecurityGroup",
        "medialive:DescribeMultiplex",
        "medialive:DescribeMultiplexProgram",
        "medialive:DescribeOffering",
        "medialive:DescribeReservation",
        "medialive:DescribeSchedule",
        "medialive:GetCloudWatchAlarmTemplate",
        "medialive:GetCloudWatchAlarmTemplateGroup",
        "medialive:GetEventBridgeRuleTemplate",
        "medialive:GetEventBridgeRuleTemplateGroup",
        "medialive:GetSignalMap",
        "medialive:ListChannels",
        "medialive:ListCloudWatchAlarmTemplateGroups",
        "medialive:ListCloudWatchAlarmTemplates",
        "medialive:ListEventBridgeRuleTemplateGroups",
        "medialive:ListEventBridgeRuleTemplates",
        "medialive:ListInputDeviceTransfers",
        "medialive:ListInputDevices",
        "medialive:ListInputSecurityGroups",
        "medialive:ListInputs",
        "medialive:ListMultiplexPrograms",
        "medialive:ListMultiplexes",
        "medialive:ListOfferings",
        "medialive:ListReservations",
        "medialive:ListSignalMaps",
        "medialive:ListTagsForResource",
        "mediapackage-vod:Describe*",
        "mediapackage-vod:List*",
        "mediapackage:Describe*",
        "mediapackage:List*",
        "mediapackagev2:GetChannel",
        "mediapackagev2:GetChannelGroup",
        "mediapackagev2:GetChannelPolicy",
        "mediapackagev2:GetHeadObject",
        "mediapackagev2:GetObject",
        "mediapackagev2:GetOriginEndpoint",
        "mediapackagev2:GetOriginEndpointPolicy",
        "mediapackagev2:ListChannelGroups",
        "mediapackagev2:ListChannels",
        "mediapackagev2:ListOriginEndpoints",
        "mediapackagev2:ListTagsForResource",
        "mediastore:DescribeContainer",
```

```
        "mediastore:DescribeObject",
        "mediastore:GetContainerPolicy",
        "mediastore:GetCorsPolicy",
        "mediastore:GetLifecyclePolicy",
        "mediastore:GetMetricPolicy",
        "mediastore:GetObject",
        "mediastore:ListContainers",
        "mediastore:ListItems",
        "mediastore:ListTagsForResource",
        "memorydb:DescribeClusters",
        "memorydb:DescribeParameterGroups",
        "memorydb:DescribeParameters",
        "memorydb:ListTags",
        "mgh:Describe*",
        "mgh:GetHomeRegion",
        "mgh:List*",
        "mgn:DescribeJobLogItems",
        "mgn:DescribeJobs",
        "mgn:DescribeLaunchConfigurationTemplates",
        "mgn:DescribeReplicationConfigurationTemplates",
        "mgn:DescribeSourceServers",
        "mgn:DescribeVcenterClients",
        "mgn:GetLaunchConfiguration",
        "mgn:GetReplicationConfiguration",
        "mgn:ListApplications",
        "mgn:ListSourceServerActions",
        "mgn:ListTemplateActions",
        "mgn:ListWaves",
        "mobileanalytics:Get*",
        "mobiletargeting:Get*",
        "mobiletargeting:List*",
        "monitron:GetProject",
        "monitron:GetProjectAdminUser",
        "monitron:ListProjects",
        "monitron:ListTagsForResource",
        "mq:Describe*",
        "mq:List*",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeLoggingConfiguration",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:DescribeRuleGroupMetadata",
        "network-firewall:DescribeTLSInspectionConfiguration",
```

```
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups",
        "network-firewall:ListTLSInspectionConfigurations",
        "network-firewall:ListTagsForResource",
        "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",
        "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:GetTelemetryEvaluationStatus",
        "observabilityadmin:GetTelemetryEvaluationStatusForOrganization",
        "observabilityadmin:ListResourceTelemetry",
        "observabilityadmin:ListResourceTelemetryForOrganization",
        "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:GetDefaultView",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:GetView",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListSupportedResourceTypes",
        "resource-explorer-2:ListTagsForResource",
        "resource-explorer-2:ListViews",
        "resource-explorer-2:Search",
        "resource-groups:Get*",
        "resource-groups:List*",
        "resource-groups:Search*",
        "robomaker:BatchDescribe*",
        "robomaker:Describe*",
        "robomaker:Get*",
        "robomaker:List*",
        "route53-recovery-cluster:Get*",
        "route53-recovery-cluster:ListRoutingControls",
        "route53-recovery-control-config:Describe*",
        "route53-recovery-control-config:GetResourcePolicy",
        "route53-recovery-control-config:List*",
        "route53-recovery-readiness:Get*",
        "route53-recovery-readiness:List*",
        "route53:Get*",
        "route53:List*",
        "route53:Test*",
        "route53domains:Check*",
        "route53domains:Get*",
        "route53domains:List*",
        "route53domains:View*",
        "route53profiles:GetProfile",
        "route53profiles:GetProfileAssociation",
        "route53profiles:GetProfileResourceAssociation",
        "route53profiles:ListProfileAssociations",
        "route53profiles:ListProfileResourceAssociations",
        "route53profiles:ListProfiles",
        "route53profiles:ListTagsForResource",
        "route53resolver:Get*",
        "route53resolver:List*",
        "rum:GetAppMonitor",
        "rum:GetAppMonitorData",
        "rum:ListAppMonitors",
        "s3-object-lambda:GetObject",
        "s3-object-lambda:GetObjectAcl",
        "s3-object-lambda:GetObjectLegalHold",
```

```
        "s3-object-lambda:GetObjectRetention",
        "s3-object-lambda:GetObjectTagging",
        "s3-object-lambda:GetObjectVersion",
        "s3-object-lambda:GetObjectVersionAcl",
        "s3-object-lambda:GetObjectVersionTagging",
        "s3-object-lambda:ListBucket",
        "s3-object-lambda:ListBucketMultipartUploads",
        "s3-object-lambda:ListBucketVersions",
        "s3-object-lambda:ListMultipartUploadParts",
        "s3-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*",
        "sagemaker-groundtruth-synthetic:GetAccountDetails",
        "sagemaker-groundtruth-synthetic:GetBatch",
        "sagemaker-groundtruth-synthetic:GetProject",
        "sagemaker-groundtruth-synthetic:ListBatchDataTransfers",
        "sagemaker-groundtruth-synthetic:ListBatchSummaries",
        "sagemaker-groundtruth-synthetic:ListProjectDataTransfers",
        "sagemaker-groundtruth-synthetic:ListProjectSummaries",
        "sagemaker:Describe*",
        "sagemaker:GetSearchSuggestions",
        "sagemaker:List*",
```

```
        "sagemaker:Search",
        "savingsplans:DescribeSavingsPlanRates",
        "savingsplans:DescribeSavingsPlans",
        "savingsplans:DescribeSavingsPlansOfferingRates",
        "savingsplans:DescribeSavingsPlansOfferings",
        "savingsplans:ListTagsForResource",
        "scheduler:GetSchedule",
        "scheduler:GetScheduleGroup",
        "scheduler:ListScheduleGroups",
        "scheduler:ListSchedules",
        "scheduler:ListTagsForResource",
        "schemas:Describe*",
        "schemas:Get*",
        "schemas:List*",
        "schemas:Search*",
        "sdb:Get*",
        "sdb:List*",
        "sdb:Select*",
        "secretsmanager:Describe*",
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:List*",
        "securityhub: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:DescribeSenderIds",
        "sms-voice:DescribeSpendLimits",
```

```
        "sms-voice:ListPoolOriginationIdentities",
        "sms-voice:ListTagsForResource",
        "snowball:Describe*",
        "snowball:Get*",
        "snowball:List*",
        "sns:Check*",
        "sns:Get*",
        "sns:List*",
        "sqs:Get*",
        "sqs:List*",
        "sqs:Receive*",
        "ssm-contacts:DescribeEngagement",
        "ssm-contacts:DescribePage",
        "ssm-contacts:GetContact",
        "ssm-contacts:GetContactChannel",
        "ssm-contacts:ListContactChannels",
        "ssm-contacts:ListContacts",
        "ssm-contacts:ListEngagements",
        "ssm-contacts:ListPageReceipts",
        "ssm-contacts:ListPagesByContact",
        "ssm-contacts:ListPagesByEngagement",
        "ssm-incidents:GetIncidentRecord",
        "ssm-incidents:GetReplicationSet",
        "ssm-incidents:GetResourcePolicies",
        "ssm-incidents:GetResponsePlan",
        "ssm-incidents:GetTimelineEvent",
        "ssm-incidents:ListIncidentRecords",
        "ssm-incidents:ListRelatedItems",
        "ssm-incidents:ListReplicationSets",
        "ssm-incidents:ListResponsePlans",
        "ssm-incidents:ListTagsForResource",
        "ssm-incidents:ListTimelineEvents",
        "ssm-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:GetDatabase",
        "ssm-sap:GetOperation",
        "ssm-sap:GetResourcePermission",
```

```
        "ssm-sap:ListApplications",
        "ssm-sap:ListComponents",
        "ssm-sap:ListDatabases",
        "ssm-sap:ListOperationEvents",
        "ssm-sap:ListOperations",
        "ssm-sap:ListTagsForResource",
        "ssm:Describe*",
        "ssm:Get*",
        "ssm:List*",
        "sso-directory:Describe*",
        "sso-directory:List*",
        "sso-directory:Search*",
        "sso:Describe*",
        "sso:Get*",
        "sso:List*",
        "sso:Search*",
        "states:Describe*",
        "states:GetExecutionHistory",
        "states:List*",
        "states:ValidateStateMachineDefinition",
        "storagegateway:Describe*",
        "storagegateway:List*",
        "sts:GetAccessKeyInfo",
        "sts:GetCallerIdentity",
        "sts:GetSessionToken",
        "support:DescribeAttachment",
        "support: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",
        "verifiedpermissions:GetIdentitySource",
        "verifiedpermissions:GetPolicy",
        "verifiedpermissions:GetPolicyStore",
        "verifiedpermissions:GetPolicyTemplate",
        "verifiedpermissions:GetSchema",
        "verifiedpermissions:IsAuthorized",
        "verifiedpermissions:IsAuthorizedWithToken",
        "verifiedpermissions:ListIdentitySources",
        "verifiedpermissions:ListPolicies",
        "verifiedpermissions:ListPolicyStores",
        "verifiedpermissions:ListPolicyTemplates",
        "vpc-lattice:GetAccessLogSubscription",
        "vpc-lattice:GetAuthPolicy",
        "vpc-lattice:GetListener",
        "vpc-lattice:GetResourcePolicy",
        "vpc-lattice:GetRule",
        "vpc-lattice:GetService",
        "vpc-lattice:GetServiceNetwork",
        "vpc-lattice:GetServiceNetworkServiceAssociation",
        "vpc-lattice:GetServiceNetworkVpcAssociation",
        "vpc-lattice:GetTargetGroup",
        "vpc-lattice:ListAccessLogSubscriptions",
        "vpc-lattice:ListListeners",
        "vpc-lattice:ListRules",
        "vpc-lattice:ListServiceNetworkServiceAssociations",
```

```
        "vpc-lattice:ListServiceNetworkVpcAssociations",
        "vpc-lattice:ListServiceNetworks",
        "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" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

ResourceGroupsandTagEditorFullAccess

Deskripsi: Menyediakan akses penuh ke Resource Groups dan Tag Editor.

`ResourceGroupsandTagEditorFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ResourceGroupsandTagEditorFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:39 UTC

- Waktu telah diedit: Agustus 10, 2023, 13:29 UTC
- ARN: `arn:aws:iam::aws:policy/ResourceGroupsandTagEditorFullAccess`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:getResources",
        "tag:getTagKeys",
        "tag:getTagValues",
        "tag:TagResources",
        "tag:UntagResources",
        "resource-groups:*",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "cloudformation:ListStacks"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

ResourceGroupsandTagEditorReadOnlyAccess

Deskripsi: Menyediakan akses untuk menggunakan Resource Groups dan Tag Editor, tetapi tidak mengizinkan pengeditan tag melalui Editor Tag.

`ResourceGroupsandTagEditorReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ResourceGroupsandTagEditorReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:39 UTC
- Waktu telah diedit: Agustus 10, 2023, 13:42 UTC
- ARN: `arn:aws:iam::aws:policy/ResourceGroupsandTagEditorReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
        "tag:getTagKeys",
        "tag:getTagValues",
        "resource-groups:Get*",
        "resource-groups:List*",
        "resource-groups:Search*",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "cloudformation:ListStacks"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

ResourceGroupsServiceRolePolicy

Deskripsi: Memungkinkan AWS Resource Groups untuk menanyakan AWS layanan yang memiliki sumber daya Anda untuk mempertahankan grup up-to-date

`ResourceGroupsServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 05 Januari 2023, 16:57 UTC
- Waktu telah diedit: 05 Januari 2023, 16:57 UTC

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

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

ResourceGroupsTaggingAPITagUntagSupportedResources

Deskripsi: Memberikan izin untuk menandai dan menghapus tag semua sumber daya yang didukung oleh Resource Groups Tagging API. Kebijakan ini juga memberikan izin yang diperlukan untuk mengambil semua sumber daya yang diberi tag, atau diberi tag sebelumnya, melalui Resource Groups Tagging API.

`ResourceGroupsTaggingAPITagUntagSupportedResources`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ResourceGroupsTaggingAPITagUntagSupportedResources` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 11 Oktober 2024, 11:11 UTC
- Waktu yang telah diedit: 11 Desember 2024, 17:51 UTC
- ARN: `arn:aws:iam::aws:policy/ResourceGroupsTaggingAPITagUntagSupportedResources`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

ROSAAmazonEBSCSIDriverOperatorPolicy

Deskripsi: Memungkinkan Operator Driver OpenShift Amazon EBS Container Storage Interface (CSI) untuk menginstal dan memelihara driver Amazon EBS CSI pada cluster Red Hat OpenShift Service on AWS (ROSA). Driver Amazon EBS CSI memungkinkan cluster ROSA untuk mengelola siklus hidup volume Amazon EBS untuk volume persisten.

`ROSAAmazonEBSCSIDriverOperatorPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ROSAAmazonEBSCSIDriverOperatorPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 20 April 2023, 22:36 UTC
- Waktu yang telah diedit: 22 Januari 2025, 00:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAAmazonEBSCSIDriverOperatorPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
```

```
        "ec2:DescribeSnapshots",
        "ec2:DescribeTags",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume",
        "ec2:ModifyVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "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"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

ROSACloudNetworkConfigOperatorPolicy

Deskripsi: Memungkinkan OpenShift Cloud Network Config Controller Operator untuk menyediakan dan mengelola sumber daya jaringan untuk digunakan oleh Red Hat OpenShift Service on AWS (ROSA) cluster networking overlay. Operator Jaringan OpenShift Cloud berinteraksi dengan AWS APIs atas nama plugin jaringan melalui. CustomResourceDefinitions Operator menggunakan izin kebijakan ini untuk mengelola alamat IP pribadi untuk EC2 instans Amazon sebagai bagian dari cluster ROSA.

`ROSACloudNetworkConfigOperatorPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ROSACloudNetworkConfigOperatorPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 20 April 2023, 22:34 UTC
- Waktu telah diedit: 20 April 2023, 22:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSACloudNetworkConfigOperatorPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeNetworkResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ModifyEIPs",
      "Effect" : "Allow",
      "Action" : [
        "ec2:UnassignPrivateIpAddresses",
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignIpv6Addresses",
        "ec2:AssignIpv6Addresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

ROSAControlPlaneOperatorPolicy

Deskripsi: Memungkinkan Red Hat OpenShift Service on AWS (ROSA) control plane untuk mengelola sumber daya ROSA cluster Amazon EC2 dan Amazon Route 53.

`ROSAControlPlaneOperatorPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ROSAControlPlaneOperatorPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 24 April 2023, 23:02 UTC
- Waktu yang telah diedit: 10 April 2025, 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAControlPlaneOperatorPolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints",
```

```
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "route53:ListHostedZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateSecurityGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "DeleteSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "SecurityGroupIngressEgress",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress"
```

```
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSecurityGroupsVPCNoCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "ListResourceRecordSets",
      "Effect" : "Allow",
      "Action" : [
        "route53:ListResourceRecordSets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ChangeResourceRecordSetsRestrictedRecordNames",
      "Effect" : "Allow",
      "Action" : [
        "route53:ChangeResourceRecordSets"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "route53:ChangeResourceRecordSetsNormalizedRecordNames" : [
            "*.hypershift.local"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "VPCEndpointWithCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "VPCEndpointResourceTagCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "VPCEndpointNoCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*"
      ]
```

```
    },
    {
      "Sid" : "ManageVPCEndpointWithCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint",
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "ModifyVPCEndpoingNoCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Sid" : "CreateTagsRestrictedActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateVpcEndpoint",
            "CreateSecurityGroup"
          ]
        }
```

```
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

ROSAImageRegistryOperatorPolicy

Deskripsi: Memungkinkan Operator Registri OpenShift Gambar untuk menyediakan dan mengelola bucket dan objek Amazon S3 untuk digunakan oleh Red Hat OpenShift Service on AWS (ROSA) in-cluster image registry untuk memenuhi persyaratan penyimpanan ROSA. OpenShift Image Registry Operator menginstal dan memelihara registri internal OpenShift cluster Red Hat.

`ROSAImageRegistryOperatorPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ROSAImageRegistryOperatorPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 27 April 2023, 20:13 UTC
- Waktu yang telah diedit: 19 Mei 2025, 18:22 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAImageRegistryOperatorPolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ListBuckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSpecificBucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:GetBucketTagging",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetBucketLocation",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketTagging",
        "s3:PutEncryptionConfiguration",
        "s3:PutLifecycleConfiguration"
      ],
      "Resource" : [
        "arn:aws:s3:::*-image-registry-${aws:RequestedRegion}-*",
        "arn:aws:s3:::*-image-registry-${aws:RequestedRegion}?",
        "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}/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

ROSAIngressOperatorPolicy

Deskripsi: Memungkinkan Operator OpenShift Ingress untuk menyediakan dan mengelola penyeimbang beban dan konfigurasi sistem nama domain (DNS) untuk kluster Red Hat OpenShift Service on AWS (ROSA). Kebijakan ini memungkinkan akses baca ke nilai tag, yang disaring operator untuk sumber daya Route 53 untuk menemukan zona yang dihosting.

`ROSAIngressOperatorPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ROSAIngressOperatorPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan

- Waktu pembuatan: 20 April 2023, 22:37 UTC
- Waktu yang telah diedit: 10 April 2025, 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAIngressOperatorPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "route53:ListHostedZones",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:ChangeResourceRecordSets"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "route53:ChangeResourceRecordSetsNormalizedRecordNames" : [
            "*.openshiftapps.com",
            "*.devshift.org",
            "*.openshiftusgov.com",
            "*.devshiftusgov.com"
          ]
        }
```

```
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

ROSAInstallerPolicy

Deskripsi: Memungkinkan penginstal Red Hat OpenShift Service on AWS (ROSA) mengelola AWS sumber daya yang mendukung instalasi klaster ROSA. Ini termasuk mengelola profil instance untuk node pekerja ROSA.

`ROSAInstallerPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ROSAInstallerPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 06 Juni 2023, 21:00 UTC
- Waktu yang telah diedit: 10 April 2025, 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAInstallerPolicy`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeRegions",
        "ec2:DescribeReservedInstancesOfferings",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:DescribeInstanceTypeOfferings",
        "elasticloadbalancing:DescribeAccountLimits",
        "elasticloadbalancing:DescribeLoadBalancers",
        "iam:GetOpenIDConnectProvider",
        "iam:GetRole",
        "route53:GetHostedZone",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName",
        "route53:ListResourceRecordSets",
        "route53:GetAccountLimit",
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassRoleToEC2",
      "Effect" : "Allow",
      "Action" : [
```

```
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:*:iam::*:role/*-ROSA-Worker-Role"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ManageInstanceProfiles",
      "Effect" : "Allow",
      "Action" : [
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:GetInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/rosa-service-managed-*"
      ]
    },
    {
      "Sid" : "CreateInstanceProfiles",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateInstanceProfile",
        "iam:TagInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/rosa-service-managed-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "GetSecretValue",
```

```
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "Route53ManageRecords",
      "Effect" : "Allow",
      "Action" : [
        "route53:ChangeResourceRecordSets"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "route53:ChangeResourceRecordSetsNormalizedRecordNames" : [
            "*.openshiftapps.com",
            "*.devshift.org",
            "*.hypershift.local",
            "*.openshiftusgov.com",
            "*.devshiftusgov.com"
          ]
        }
      }
    },
    {
      "Sid" : "Route53Manage",
      "Effect" : "Allow",
      "Action" : [
        "route53:ChangeTagsForResource",
        "route53:CreateHostedZone",
        "route53:DeleteHostedZone"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateTags",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances"
          ]
        }
      }
    },
    {
      "Sid" : "RunInstancesNoCondition",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:snapshot/*"
      ]
    },
    {
      "Sid" : "RunInstancesRestrictedRequestTag",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "RunInstancesRedHatOwnedAMIs",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:image/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:Owner" : [
            "531415883065",
            "251351625822",
            "210686502322"
          ]
        }
      }
    },
    {
      "Sid" : "ManageInstancesRestrictedResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances",
        "ec2:GetConsoleOutput"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateGrantRestrictedResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com"
        },
```

```
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        }
      }
    },
    {
      "Sid" : "ManagedKMSRestrictedResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSecurityGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "DeleteSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "SecurityGroupIngressEgress",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSecurityGroupsVPCNoCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "CreateTagsRestrictedActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "ec2:CreateAction" : [
            "CreateSecurityGroup"
          ]
        }
      }
    },
    {
      "Sid" : "CreateTagsK8sSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "kubernetes.io/cluster/*"
          ]
        }
      }
    },
    {
      "Sid" : "ListPoliciesAttachedToRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

ROSAKMSProviderPolicy

Deskripsi: Memungkinkan Penyedia AWS Enkripsi ROSA bawaan untuk mengelola AWS kunci Layanan Manajemen Kunci (KMS) untuk mendukung enkripsi data etcd menggunakan kunci KMS yang disediakan AWS pelanggan. Kebijakan ini memungkinkan enkripsi dan dekripsi data menggunakan kunci KMS.

`ROSAKMSProviderPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ROSAKMSProviderPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 27 April 2023, 20:10 UTC
- Waktu telah diedit: 27 April 2023, 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAKMSProviderPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      "Sid" : "VolumeEncryption",
      "Effect" : "Allow",
      "Action" : [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

ROSAKubeControllerPolicy

Deskripsi: Memungkinkan pengontrol ROSA Kubernetes mengelola sumber daya Amazon, Elastic Load EC2 Balancing (ELB), dan AWS Key Management Service (KMS) untuk klaster ROSA.

`ROSAKubeControllerPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ROSAKubeControllerPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 27 April 2023, 20:09 UTC

- Waktu yang telah diedit: 10 April 2025, 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAKubeControllerPolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInstances",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeLoadBalancerPolicies"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "KMSDescribeKey",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
```

```
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        }
      }
    },
    {
      "Sid" : "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"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

ROSAManageSubscription

Deskripsi: Kebijakan ini memberikan izin yang diperlukan untuk mengelola langganan Red Hat OpenShift Service on AWS (ROSA).

`ROSAManageSubscription`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ROSAManageSubscription` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 11 April 2022, 20:58 UTC
- Waktu telah diedit: 04 Agustus 2023, 19:59 UTC
- ARN: `arn:aws:iam::aws:policy/ROSAManageSubscription`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:Subscribe",
        "aws-marketplace:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws-marketplace:ProductId" : [
            "34850061-abaf-402d-92df-94325c9e947f",
            "bfdca560-2c78-4e64-8193-794c159e6d30"
          ]
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ViewSubscriptions"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

ROSANodePoolManagementPolicy

Deskripsi: Memungkinkan Red Hat OpenShift Service on AWS (ROSA) untuk mengelola EC2 instance klaster sebagai node pekerja, termasuk izin untuk mengonfigurasi grup keamanan dan menandai instance dan volume. Kebijakan ini juga memungkinkan penggunaan EC2 instance dengan enkripsi disk yang disediakan oleh AWS kunci Key Management Service (KMS).

`ROSANodePoolManagementPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ROSANodePoolManagementPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 08 Juni 2023, 20:48 UTC
- Waktu telah diedit: 05 Mei 2025, 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSANodePoolManagementPolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

ROSASRESupportPolicy

Deskripsi: Menyediakan rekayasa keandalan situs ROSA (SRE) izin yang diperlukan untuk mengamati, mendiagnosis, dan mendukung AWS sumber daya yang terkait dengan kluster Red Hat OpenShift Service on AWS (ROSA), termasuk kemampuan untuk mengubah status node cluster ROSA.

`ROSASRESupportPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ROSASRESupportPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 01 Juni 2023, 14:36 UTC
- Waktu yang telah diedit: 10 April 2025, 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSASRESupportPolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeRegions",
        "sts:DecodeAuthorizationMessage"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Route53",
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
        "route53:GetHostedZoneCount",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName",
        "route53:ListResourceRecordSets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "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"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

ROSAWorkerInstancePolicy

Deskripsi: Mengizinkan node pekerja Red Hat OpenShift Service on AWS (ROSA) di akun Anda akses hanya-baca ke EC2 instans Amazon dan Wilayah AWS untuk manajemen siklus hidup node komputasi.

`ROSAWorkerInstancePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ROSAWorkerInstancePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 20 April 2023, 22:35 UTC
- Waktu telah diedit: 20 Maret 2025, 23:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAWorkerInstancePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

Route53RecoveryReadinessServiceRolePolicy

Deskripsi: Kebijakan Peran Tertaut Layanan untuk Kesiapan Pemulihan Route 53

`Route53RecoveryReadinessServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 15 Juli 2021, 16:06 UTC
- Waktu yang telah diedit: 14 Februari 2023, 18:08 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Route53RecoveryReadinessServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeReservedCapacity",
        "dynamodb:DescribeReservedCapacityOfferings"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeTable",
        "dynamodb:DescribeTimeToLive"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/servicequotas.amazonaws.com/
AWSServiceRoleForServiceQuotas",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "servicequotas.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetFunctionConcurrency",
        "lambda:GetFunctionConfiguration",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:ListProvisionedConcurrencyConfigs",
        "lambda:ListAliases",
        "lambda:ListVersionsByFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBClusters"
      ],
      "Resource" : "arn:aws:rds:*:*:cluster:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "rds:DescribeDBInstances"
      ],
      "Resource" : "arn:aws:rds:*:*:db:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:ListResourceRecordSets"
      ],
      "Resource" : "arn:aws:route53:::hostedzone/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHealthCheck",
        "route53:GetHealthCheckStatus"
      ],
      "Resource" : "arn:aws:route53:::healthcheck/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:RequestServiceQuotaIncrease"
      ],
      "Resource" : "arn:aws:servicequotas:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:GetTopicAttributes",
        "sns:ListSubscriptionsByTopic"
      ],
      "Resource" : "arn:aws:sns:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl"
      ],
      "Resource" : "arn:aws:sqs:*:*:*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "apigateway:GET",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "autoscaling:DescribeAccountLimits",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeLifecycleHooks",
        "autoscaling:DescribeLoadBalancers",
        "autoscaling:DescribeLoadBalancerTargetGroups",
        "autoscaling:DescribeNotificationConfigurations",
        "autoscaling:DescribePolicies",
        "cloudwatch:GetMetricData",
        "cloudwatch:DescribeAlarms",
        "dynamodb:DescribeLimits",
        "dynamodb:ListGlobalTables",
        "dynamodb:ListTables",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetEbsDefaultKmsKeyId",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "kafka:DescribeCluster",
        "kafka:DescribeConfigurationRevision",
        "lambda:ListEventSourceMappings",
        "lambda:ListFunctions",
        "rds:DescribeAccountAttributes",
        "route53:GetHostedZone",
        "servicequotas:ListAWSDefaultServiceQuotas",
        "servicequotas:ListRequestedServiceQuotaChangeHistory",
        "servicequotas:ListServiceQuotas",
        "servicequotas:ListServices",
        "sns:GetEndpointAttributes",
        "sns:GetSubscriptionAttributes"
```

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

Route53ResolverServiceRolePolicy

Deskripsi: Mengaktifkan akses ke Layanan AWS dan Sumber Daya yang digunakan atau dikelola oleh Route53 Resolver

`Route53ResolverServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 12 Agustus 2020, 17:47 UTC
- Waktu yang telah diedit: 12 Agustus 2020, 17:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Route53ResolverServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

S3StorageLensServiceRolePolicy

Deskripsi: Mengaktifkan akses ke Layanan AWS dan Sumber Daya yang digunakan atau dikelola oleh S3 Storage Lens

`S3StorageLensServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 18 November 2020, 18:15 UTC
- Waktu yang telah diedit: 18 November 2020, 18:15 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/S3StorageLensServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AwsOrgsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : [
        "*"
      ]
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

SageMakerStudioAdminProjectUserRolePolicy

Deskripsi: Kebijakan IAM ini memberikan peran IAM akses penuh ke AWS Glue Data Catalog (metadata) dan Amazon S3 (data aktual) untuk operasi data lake, dengan akses yang dicakup berdasarkan akun, dan tag peran.

`SageMakerStudioAdminProjectUserRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `SageMakerStudioAdminProjectUserRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 09 Juli 2025, 20:52 UTC
- Waktu yang telah diedit: 09 Juli 2025, 20:52 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioAdminProjectUserRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

SageMakerStudioBedrockAgentServiceRolePolicy

Deskripsi: Memungkinkan Agen Amazon Bedrock mengakses model Amazon Bedrock dan sumber daya lain yang dilampirkan ke agen di SageMaker Studio.

`SageMakerStudioBedrockAgentServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `SageMakerStudioBedrockAgentServiceRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan

- Waktu pembuatan: 13 Februari 2025, 23:37 UTC
- Waktu telah diedit: 13 Februari 2025, 23:37 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockAgentServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

SageMakerStudioBedrockChatAgentUserRolePolicy

Deskripsi: Menyediakan akses ke konfigurasi aplikasi agen obrolan Amazon Bedrock dan agen Amazon Bedrock di SageMaker Studio.

`SageMakerStudioBedrockChatAgentUserRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `SageMakerStudioBedrockChatAgentUserRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 13 Februari 2025, 23:52 UTC
- Waktu yang telah diedit: 13 Februari 2025, 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockChatAgentUserRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

SageMakerStudioBedrockEvaluationJobServiceRolePolicy

Deskripsi: Memungkinkan Amazon Bedrock mengakses model dan kumpulan data Amazon Bedrock untuk pekerjaan evaluasi di Studio. SageMaker

`SageMakerStudioBedrockEvaluationJobServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `SageMakerStudioBedrockEvaluationJobServiceRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 14 Februari 2025, 00:37 UTC
- Waktu yang telah diedit: 14 Februari 2025, 00:37 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockEvaluationJobServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

SageMakerStudioBedrockFlowServiceRolePolicy

Deskripsi: Memungkinkan Amazon Bedrock Flows mengakses model Amazon Bedrock dan sumber daya lain yang dilampirkan ke aliran di SageMaker Studio.

`SageMakerStudioBedrockFlowServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `SageMakerStudioBedrockFlowServiceRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 14 Februari 2025, 00:07 UTC
- Waktu telah diedit: 09 April 2025, 20:37 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockFlowServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

SageMakerStudioBedrockFunctionExecutionRolePolicy

Deskripsi: Memungkinkan AWS Lambda mengakses konfigurasi komponen fungsi Amazon Bedrock di Studio. SageMaker

`SageMakerStudioBedrockFunctionExecutionRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `SageMakerStudioBedrockFunctionExecutionRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 25 Februari 2025, 03:52 UTC
- Waktu telah diedit: 25 Februari 2025, 03:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockFunctionExecutionRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

SageMakerStudioBedrockKnowledgeBaseCustomResourcePolicy

Deskripsi: Menyediakan akses untuk mengonfigurasi penyimpanan vektor dan basis pengetahuan Amazon Bedrock di SageMaker Studio.

`SageMakerStudioBedrockKnowledgeBaseCustomResourcePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `SageMakerStudioBedrockKnowledgeBaseCustomResourcePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 25 Februari 2025, 03:37 UTC
- Waktu telah diedit: 25 Februari 2025, 03:37 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockKnowledgeBaseCustomResourcePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy

Deskripsi: Memungkinkan Pangkalan Pengetahuan Amazon Bedrock mengakses model dan sumber data Amazon Bedrock di SageMaker Studio.

`SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 25 Februari 2025, 02:52 UTC
- Waktu telah diedit: 16 April 2025, 20:37 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

SageMakerStudioBedrockPromptUserRolePolicy

Deskripsi: Menyediakan akses ke prompt Amazon Bedrock dan konfigurasinya di SageMaker Studio.

`SageMakerStudioBedrockPromptUserRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `SageMakerStudioBedrockPromptUserRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 14 Februari 2025, 00:22 UTC
- Waktu yang telah diedit: 14 Februari 2025, 00:22 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockPromptUserRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

SageMakerStudioDomainExecutionRolePolicy

Deskripsi: Kebijakan ini digunakan oleh Amazon SageMaker Studio untuk membuat katalog, menemukan, mengatur, berbagi, dan menganalisis data di domain Amazon SageMaker Studio.

`SageMakerStudioDomainExecutionRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `SageMakerStudioDomainExecutionRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 20 November 2024, 21:56 UTC
- Waktu yang telah diedit: 17 Juni 2025, 20:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioDomainExecutionRolePolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataZonePermissions",
      "Effect" : "Allow",
      "Action" : [
        "datazone:AcceptPredictions",
        "datazone:AcceptSubscriptionRequest",
        "datazone:AddEntityOwner",
        "datazone:AddPolicyGrant",
        "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: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/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

SageMakerStudioDomainServiceRolePolicy

Deskripsi: Peran layanan untuk tindakan tingkat domain di portal yang dilakukan oleh Amazon SageMaker Studio.

`SageMakerStudioDomainServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `SageMakerStudioDomainServiceRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 20 November 2024, 21:56 UTC
- Waktu telah diedit: 20 November 2024, 21:56 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioDomainServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

SageMakerStudioEMRInstanceRolePolicy

Deskripsi: Amazon SageMaker Studio membuat peran IAM bagi pengguna proyek untuk melakukan analisis data, kecerdasan buatan, dan tindakan pembelajaran mesin, serta menggunakan kebijakan ini saat membuat peran ini untuk menentukan izin yang terkait dengan EMR.

`SageMakerStudioEMRInstanceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `SageMakerStudioEMRInstanceRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 27 Februari 2025, 00:22 UTC
- Waktu yang telah diedit: 27 Februari 2025, 00:22 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioEMRInstanceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

SageMakerStudioEMRServiceRolePolicy

Deskripsi: Amazon SageMaker Studio membuat peran IAM bagi pengguna proyek untuk melakukan analisis data, kecerdasan buatan, dan tindakan pembelajaran mesin, serta menggunakan kebijakan ini saat membuat peran ini untuk menentukan izin yang terkait dengan EMR.

`SageMakerStudioEMRServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `SageMakerStudioEMRServiceRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan

- Waktu pembuatan: 31 Januari 2025, 19:52 UTC
- Waktu yang telah diedit: 27 Februari 2025, 00:22 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioEMRServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "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/${aws:PrincipalTag/VpcId}"
        }
      }
    },
    {
      "Sid" : "EMRKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:ReEncryptFrom",
        "kms:ReEncryptTo",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${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" : "AllowEMRForKMSManagement",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListGrants",
        "kms:RevokeGrant",
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowEMRToListKmsAliases",
      "Effect" : "Allow",
      "Action" : "kms:ListAliases",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

SageMakerStudioFullAccess

Deskripsi: Kebijakan ini menyediakan akses penuh ke Amazon SageMaker Unified Studio melalui konsol SageMaker manajemen Amazon.

`SageMakerStudioFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `SageMakerStudioFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 November 2024, 00:06 UTC
- Waktu yang telah diedit: 06 Juni 2025, 19:07 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioFullAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
  "Statement" : [
    {
      "Sid" : "AmazonDataZoneStatement",
      "Effect" : "Allow",
      "Action" : [
        "datazone:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ReadOnlyStatement",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "iam:ListRoles",
        "sso:DescribeRegisteredRegions",
        "s3:ListAllMyBuckets",
        "redshift:DescribeClusters",
        "redshift-serverless:ListWorkgroups",
        "ec2: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"
      ],
      "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/*",
        "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" : [
        "*"
      ]
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

SageMakerStudioProjectProvisioningRolePolicy

Deskripsi: Amazon SageMaker Studio menggunakan kebijakan ini untuk menyediakan dan mengelola sumber daya di akun Anda.

`SageMakerStudioProjectProvisioningRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `SageMakerStudioProjectProvisioningRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 20 November 2024, 21:58 UTC
- Waktu yang telah diedit: 03 Juli 2025, 18:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioProjectProvisioningRolePolicy`

Versi kebijakan

Versi kebijakan: v16 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "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"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DzTemplate",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DzCfTemplate",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::amazon-sagemaker-cf-templates*/*"
    },
    {
      "Sid" : "CcCreate",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:CreateRepository",
        "codecommit:TagResource"
      ],
      "Resource" : "arn:aws:codecommit:*:*:datazone*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
```

```
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        }
      }
    },
    {
      "Sid" : "CcDelete",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:DeleteRepository",
        "codecommit:UpdateRepositoryEncryptionKey",
        "codecommit:PutRepositoryTriggers"
      ],
      "Resource" : "arn:aws:codecommit:*:*:datazone*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com",
          "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*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com"
```

```
        }
      }
    },
    {
      "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" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com",
          "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" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "IamManage",
      "Effect" : "Allow",
      "Action" : [
        "iam:DetachRolePolicy",
        "iam:AttachRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com"
        },
        "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/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" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com"
        },
        "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" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "AmazonBedrockManaged",
            "RedshiftDb*",
            "EnableAmazonBedrockPermissions",
            "EnableAmazonBedrockIDEPermissions",
            "EnableGlueWorkloadsPermissions",
            "EnableSageMakerMLWorkloadsPermissions",
            "DomainBucketName",
            "KmsKeyId",
            "LogGroupName",
            "RoleName",
            "vpcArn",
            "VpcId",
            "CreatedForUseWithSageMakerStudio",
            "SageMakerStudioQueryExecutionRole"
          ]
        }
      }
    },
    {
      "Sid" : "IamTagBR",
      "Effect" : "Allow",
      "Action" : [
        "iam:TagRole",
        "iam:UntagRole"
      ],
      "Resource" : "arn:aws:iam::*:role/AmazonBedrock*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com"
```

```
        },
        "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_*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com"
        },
        "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" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "EnableAmazonBedrockIDEPermissions"
        }
      }
```

```
    },
    {
      "Sid" : "ManageRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole",
        "iam:ListRolePolicies",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*",
        "arn:aws:iam::*:role/AmazonBedrock*",
        "arn:aws:iam::*:role/BedrockStudio*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com"
        },
        "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"
      ],
      "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_*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com"
        }
      }
    },
    {
      "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" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com",
          "iam:PassedToService" : [
            "elasticmapreduce.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PassRoleForEmrIP",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/datazone_emr_ec2_instance_role_*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com",
          "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" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com",
          "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" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com",
          "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" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com",
          "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" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CfnGlueDb",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:database/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueDbTag",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:catalog"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueDbDelete",
      "Effect" : "Allow",
      "Action" : [
        "glue:DeleteDatabase"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueTag",
      "Effect" : "Allow",
      "Action" : [
        "glue:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:RequestTag/AmazonDataZoneProject" : "false",
          "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}",
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com"
        }
      }
    },
    {
      "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" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "kms:EncryptionContext:glue_catalog_id" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "glue.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "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*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "cloudformation.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "LambdaManage",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:DeleteFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:athenafederatedcatalog*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:CalledViaLast" : "cloudformation.amazonaws.com"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "LambdaGet",
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:athenafederatedcatalog*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${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}",
          "aws:CalledViaLast" : "cloudformation.amazonaws.com"
        },
        "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:CalledViaLast" : [
            "glue.amazonaws.com"
          ],
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "s3:prefix" : "true"
        }
      }
    },
    {
      "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"
      ],
      "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" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RSManage",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:CreateNamespace",
        "redshift-serverless:CreateWorkgroup",
        "redshift-serverless:DeleteNamespace",
        "redshift-serverless:DeleteWorkgroup",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*",
        "arn:aws:redshift-serverless:*:*:workgroup/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${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:RequestTag/AmazonDataZoneProject" : "false",
          "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" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com"
        },
        "Null" : {
          "aws:TagKeys" : "true"
        }
      }
    },
    {
      "Sid" : "SGAuth",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
```

```
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com",
          "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/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com"
        }
      }
    },
    {
      "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:CalledViaFirst" : "cloudformation.amazonaws.com",
          "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" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com"
        }
      }
    },
    {
      "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:CalledViaFirst" : "cloudformation.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:RequestTag/AmazonDataZoneProject" : "false",
          "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:CalledViaFirst" : "cloudformation.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ManageLG",
      "Effect" : "Allow",
      "Action" : [
        "logs:DeleteLogGroup",
        "logs:DeleteRetentionPolicy",
        "logs:GetDataProtectionPolicy",
        "logs:PutDataProtectionPolicy",
        "logs:DeleteDataProtectionPolicy",
        "logs:AssociateKmsKey",
        "logs:DisassociateKmsKey",
        "logs:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:datazone-*",
        "arn:aws:logs:*:*:log-group:/aws/lambda/amazon-bedrock-ide-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "AthenaManage",
      "Effect" : "Allow",
      "Action" : [
        "athena:CreateWorkGroup",
        "athena:TagResource"
      ],
      "Resource" : "arn:aws:athena:*:*:workgroup/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        }
      }
    },
    {
      "Sid" : "AthenaWGDelete",
      "Effect" : "Allow",
      "Action" : [
        "athena:DeleteWorkGroup",
        "athena:GetWorkGroup"
      ],
      "Resource" : "arn:aws:athena:*:*:workgroup/*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com",
          "aws:ResourceAccount" : "${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:CalledViaFirst" : "cloudformation.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        }
      }
    },
    {
      "Sid" : "TagRSS",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*",
        "arn:aws:redshift-serverless:*:*:workgroup/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com",
          "aws:ResourceAccount" : "${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" : "DescribeSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "DescribeSecrets",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret"
      ],
      "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/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"
      ]
    },
    {
      "Sid" : "RedshiftList",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "redshift:GetResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com"
        }
      }
    },
    {
      "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:CalledViaFirst" : "cloudformation.amazonaws.com",
          "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" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContext:aws:redshift-serverless:arn" : "false"
        }
      }
    },
    {
      "Sid" : "GetRandom",
      "Effect" : "Allow",
      "Action" : "secretsmanager:GetRandomPassword",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "BRSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:CreateSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:PutResourcePolicy",
        "secretsmanager:DeleteResourcePolicy",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:amazon-bedrock-ide/*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com",
          "aws:ResourceAccount" : "${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:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ],
          "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:CreateDomain",
        "sagemaker:AddTags"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:domain/*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:RequestTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "ManageSMD",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:UpdateDomain",
        "sagemaker:DeleteDomain"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:domain/*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "SMDManage",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListDomains",
        "sagemaker:DescribeDomain"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com"
        }
      }
    },
    {
      "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" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "EmrSCreate",
      "Effect" : "Allow",
      "Action" : [
        "emr-serverless:CreateApplication",
        "emr-serverless:TagResource"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com",
          "aws:ResourceAccount" : "${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:CalledViaFirst" : "cloudformation.amazonaws.com",
          "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" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com"
        },
        "StringLikeIfExists" : {
          "aoss:collection" : "bedrock-ide-*",
          "aoss:index" : "bedrock-ide-*"
        }
      }
    },
    {
      "Sid" : "ManageAossPolicies",
      "Effect" : "Allow",
      "Action" : [
        "aoss:GetSecurityPolicy",
        "aoss:CreateSecurityPolicy",
        "aoss:DeleteSecurityPolicy",
        "aoss:UpdateSecurityPolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com"
        },
        "StringLikeIfExists" : {
```

```
          "aoss:collection" : "bedrock-ide-*"
        }
      }
    },
    {
      "Sid" : "GetAoss",
      "Effect" : "Allow",
      "Action" : "aoss:BatchGetCollection",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AossCollections",
      "Effect" : "Allow",
      "Action" : [
        "aoss:CreateCollection",
        "aoss:UpdateCollection",
        "aoss:DeleteCollection",
        "aoss:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "GetBedrockCfnResourceDefinitionS3",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::*/dzd*/*/genAI/*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com",
          "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:CalledViaFirst" : "cloudformation.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "ManageBRLambda",
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetFunction",
        "lambda:ListTags",
        "lambda:RemovePermission"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:amazon-bedrock-ide-*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRManage",
```

```
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:CreateSecurityConfiguration",
        "elasticmapreduce:DeleteSecurityConfiguration"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com"
        }
      }
    },
    {
      "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" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com"
        },
        "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" : "AirflowKmsCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "airflow.*.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",
      "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" : "${aws:PrincipalAccount}",
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ScheduleGroup",
      "Effect" : "Allow",
      "Action" : "scheduler:DeleteScheduleGroup",
      "Resource" : "arn:aws:scheduler:*:*:schedule-group/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
```

```
      }
    },
    {
      "Sid" : "CreateSchedule",
      "Effect" : "Allow",
      "Action" : "scheduler:CreateScheduleGroup",
      "Resource" : "arn:aws:scheduler:*:*:schedule-group/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com"
        },
        "Null" : {
          "aws:RequestTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "AmazonDataZone*"
        }
      }
    },
    {
      "Sid" : "TagSchedule",
      "Effect" : "Allow",
      "Action" : "scheduler:TagResource",
      "Resource" : "arn:aws:scheduler:*:*:schedule-group/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com"
        },
        "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" : "${aws:PrincipalAccount}",
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "ManageQSFolder",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:CreateDataSource",
        "quicksight:CreateFolder",
        "quicksight:CreateFolderMembership",
        "quicksight:CreateVPCConnection",
        "quicksight:DeleteDataSource",
        "quicksight:DeleteFolder",
        "quicksight:DescribeDataSource",
        "quicksight:DescribeFolderPermissions",
        "quicksight:DescribeDataSourcePermissions",
        "quicksight:DeleteVPCConnection",
        "quicksight:ListFolderMembers",
        "quicksight:ListTagsForResource",
        "quicksight:UpdateDataSource",
        "quicksight:UpdateDataSourcePermissions",
        "quicksight:UpdateFolder",
        "quicksight:UpdateFolderPermissions",
        "quicksight:UpdateVPCConnection"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${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}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

SageMakerStudioProjectRoleMachineLearningPolicy

Deskripsi: Amazon SageMaker Studio membuat peran IAM untuk memproyeksikan pengguna untuk melakukan analisis data, kecerdasan buatan, dan tindakan pembelajaran mesin, serta menggunakan kebijakan ini saat membuat peran ini untuk menentukan izin yang terkait dengannya. SageMaker

`SageMakerStudioProjectRoleMachineLearningPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `SageMakerStudioProjectRoleMachineLearningPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 20 November 2024, 21:55 UTC
- Waktu yang telah diedit: 14 April 2025, 21:52 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioProjectRoleMachineLearningPolicy`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

SageMakerStudioProjectUserRolePermissionsBoundary

Deskripsi: Amazon SageMaker membuat peran IAM bagi pengguna Projects untuk melakukan analisis data, kecerdasan buatan, dan tindakan pembelajaran mesin, serta menggunakan kebijakan ini saat membuat peran ini untuk menentukan batas izin mereka.

`SageMakerStudioProjectUserRolePermissionsBoundary`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `SageMakerStudioProjectUserRolePermissionsBoundary` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 20 November 2024, 21:57 UTC
- Waktu telah diedit: 03 Januari 2025, 00:37 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioProjectUserRolePermissionsBoundary`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

SageMakerStudioProjectUserRolePolicy

Deskripsi: Amazon SageMaker Studio membuat peran IAM bagi pengguna proyek untuk melakukan analisis data, kecerdasan buatan, dan tindakan pembelajaran mesin, serta menggunakan kebijakan ini saat membuat peran ini untuk menentukan izin.

`SageMakerStudioProjectUserRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `SageMakerStudioProjectUserRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 20 November 2024, 21:59 UTC
- Waktu telah diedit: 25 Juni 2025, 04:22 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioProjectUserRolePolicy`

Versi kebijakan

Versi kebijakan: v14 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "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"
      ],
      "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" : "GlueVisualETLPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "glue:GetGeneratedCode"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueCompletionsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:StartCompletion",
        "glue:GetCompletion"
      ],
      "Resource" : "arn:aws:glue:*:*:completion/*"
    },
    {
      "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/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "glue.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "kms:EncryptionContext:glue_catalog_id" : "${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" : "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" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagS3ObjectPermissionsForBedrockEvaluation",
      "Effect" : "Allow",
      "Action" : "s3:PutObjectTagging",
      "Resource" : "arn:aws:s3:::${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" : "ListLogGroupsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    },
    {
      "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: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"
      ],
```

```
      "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" : "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"
          ],
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SQLWorkBenchActionsWithoutResourceType",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:PutTab",
        "sqlworkbench:DeleteTab",
        "sqlworkbench:DriverExecute",
        "sqlworkbench:GetUserInfo",
        "sqlworkbench:ListTabs",
        "sqlworkbench:GetAutocompletionMetadata",
        "sqlworkbench:GetAutocompletionResource",
        "sqlworkbench:PassAccountSettings",
        "sqlworkbench:ListQueryExecutionHistory",
        "sqlworkbench:GetQueryExecutionHistory",
        "sqlworkbench:CreateConnection",
        "sqlworkbench:PutQCustomContext",
        "sqlworkbench:GetQCustomContext",
        "sqlworkbench:DeleteQCustomContext",
        "sqlworkbench:GetQSqlRecommendations",
        "sqlworkbench:GetQSqlPromptQuotas",
        "sqlworkbench:GetSchemaInference"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftDataActionsIAMSessionRestriction",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:DescribeStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:CancelStatement",
        "redshift-data:ListStatements"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "redshift-data:statement-owner-iam-userid" : "${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" : "RedshiftGetCredentials",
      "Effect" : "Allow",
      "Action" : [
        "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"
        },
        "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" : "EMRPersistentAppUI",
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "elasticmapreduce:GetPersistentAppUIPresignedURL"
      ],
      "Condition" : {
        "ArnLike" : {
          "elasticmapreduce:ExecutionRoleArn" : "arn:aws:iam::*:role/
${aws:PrincipalTag/RoleName}"
        }
      }
    },
    {
      "Sid" : "KmsWithEncryptPermissions",
      "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" : "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" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "KmsManagementPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListGrants",
        "kms:RevokeGrant",
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${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" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "AwsOwnedKmsManagementPermissions",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:kms:*:*:key/*"
      ],
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "sqs.*.amazonaws.com",
            "sagemaker.*.amazonaws.com"
          ]
        },
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ListKMSPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EC2PermissionsForNotebookExecution",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceTypes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "InvokeBedrockModelPermissions",
      "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",
        "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*"
          ]
        }
      }
    },
    {
      "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"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

SageMakerStudioQueryExecutionRolePolicy

Deskripsi: Amazon SageMaker Studio menggunakan kebijakan ini saat menjalankan eksekusi kueri pada koneksi federasi.

`SageMakerStudioQueryExecutionRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `SageMakerStudioQueryExecutionRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 31 Januari 2025, 19:52 UTC
- Waktu telah diedit: 31 Januari 2025, 19:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioQueryExecutionRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

SecretsManagerReadWrite

Deskripsi: Menyediakan akses baca/tulis ke AWS Secrets Manager melalui file. AWS Management Console Catatan: ini tidak termasuk tindakan IAM, jadi gabungkan dengan IAMFull Access jika konfigurasi rotasi diperlukan.

`SecretsManagerReadWrite`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `SecretsManagerReadWrite` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 04 April 2018, 18:05 UTC
- Waktu telah diedit: 22 Februari 2024, 18:12 UTC
- ARN: `arn:aws:iam::aws:policy/SecretsManagerReadWrite`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BasePermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:*",
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStacks",
        "cloudformation:ExecuteChangeSet",
        "docdb-elastic:GetCluster",
        "docdb-elastic:ListClusters",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListKeys",
        "lambda:ListFunctions",
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstances",
        "redshift:DescribeClusters",
        "redshift-serverless:ListWorkgroups",
        "redshift-serverless:GetNamespace",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LambdaPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "lambda:AddPermission",
        "lambda:CreateFunction",
        "lambda:GetFunction",
        "lambda:InvokeFunction",
        "lambda:UpdateFunctionConfiguration"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:SecretsManager*"
    },
    {
      "Sid" : "SARPermissions",
      "Effect" : "Allow",
      "Action" : [
        "serverlessrepo:CreateCloudFormationChangeSet",
        "serverlessrepo:GetApplication"
      ],
      "Resource" : "arn:aws:serverlessrepo:*:*:applications/SecretsManager*"
    },
    {
      "Sid" : "S3Permissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::awsserverlessrepo-changesets*",
        "arn:aws:s3:::secrets-manager-rotation-apps-*/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

SecurityAudit

Deskripsi: Template audit keamanan memberikan akses untuk membaca metadata konfigurasi keamanan. Ini berguna untuk perangkat lunak yang mengaudit konfigurasi file. Akun AWS

`SecurityAudit`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `SecurityAudit` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu yang telah diedit: 02 Juli 2025, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/SecurityAudit`

Versi kebijakan

Versi kebijakan: v52 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BaseSecurityAuditStatement",
      "Effect" : "Allow",
      "Action" : [
        "a4b:ListSkills",
        "access-analyzer:GetAnalyzedResource",
        "access-analyzer:GetAnalyzer",
        "access-analyzer:GetArchiveRule",
        "access-analyzer:GetFinding",
```

```
        "access-analyzer:ListAnalyzedResources",
        "access-analyzer:ListAnalyzers",
        "access-analyzer:ListArchiveRules",
        "access-analyzer:ListFindings",
        "access-analyzer:ListTagsForResource",
        "account:GetAlternateContact",
        "account: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:GetCustomModel",
        "bedrock:GetModelInvocationLoggingConfiguration",
        "bedrock:ListCustomModels",
        "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:GetEbsEncryptionByDefault",
        "ec2:GetImageBlockPublicAccessState",
        "ec2:GetManagedPrefixListAssociations",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetNetworkInsightsAccessScopeAnalysisFindings",
        "ec2:GetNetworkInsightsAccessScopeContent",
        "ec2:GetTransitGatewayAttachmentPropagations",
        "ec2:GetTransitGatewayMulticastDomainAssociations",
        "ec2:GetTransitGatewayPrefixListReferences",
        "ec2:GetTransitGatewayRouteTableAssociations",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:SearchTransitGatewayRoutes",
        "ecr-public:DescribeImages",
        "ecr-public:DescribeImageTags",
        "ecr-public:DescribeRegistries",
        "ecr-public:DescribeRepositories",
        "ecr-public:GetRegistryCatalogData",
        "ecr-public:GetRepositoryCatalogData",
        "ecr-public:GetRepositoryPolicy",
        "ecr-public:ListTagsForResource",
        "ecr:BatchGetRepositoryScanningConfiguration",
        "ecr:DescribeImages",
```

```
        "ecr:DescribeImageScanFindings",
        "ecr:DescribeRegistry",
        "ecr:DescribeRepositories",
        "ecr:GetLifecyclePolicy",
        "ecr:GetRegistryPolicy",
        "ecr:GetRegistryScanningConfiguration",
        "ecr:GetRepositoryPolicy",
        "ecr:ListImages",
        "ecr:ListTagsForResource",
        "ecs:Describe*",
        "ecs:List*",
        "eks:DescribeCluster",
        "eks:DescribeFargateProfile",
        "eks:DescribeNodeGroup",
        "eks:ListClusters",
        "eks:ListFargateProfiles",
        "eks:ListNodeGroups",
        "eks: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*",
        "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:GetObjectVersionAcl",
        "s3:GetReplicationConfiguration",
        "s3:GetStorageLensGroup",
        "s3:GetStorageLensConfiguration",
        "s3:ListAccessPoints",
        "s3:ListAllMyBuckets",
        "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:DescribePermissionsPolicies",
        "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"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

SecurityLakeResourceManagementServiceRolePolicy

Deskripsi: Menyediakan akses untuk mengelola sumber daya yang dibuat oleh Security Lake.

`SecurityLakeResourceManagementServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 14 November 2024, 22:10 UTC
- Waktu telah diedit: 14 November 2024, 22:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/SecurityLakeResourceManagementServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "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" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowListLambdaEventSourceMappings",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListEventSourceMappings"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowUpdateLambdaEventSourceMapping",
      "Effect" : "Allow",
      "Action" : [
        "lambda:UpdateEventSourceMapping"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "lambda:FunctionArn" :
 "arn:aws:lambda:*:*:function:AmazonSecurityLakeMetastoreManager-*-*"
        }
      }
    },
    {
      "Sid" : "AllowUpdateLambdaConfigs",
      "Effect" : "Allow",
      "Action" : [
        "lambda:UpdateFunctionConfiguration"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:AmazonSecurityLakeMetastoreManager-*-
*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${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}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

SecurityLakeServiceLinkedRole

Deskripsi: Kebijakan ini memberikan izin untuk mengoperasikan layanan Amazon Security Lake atas nama Anda

`SecurityLakeServiceLinkedRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 29 November 2022, 14:03 UTC
- Waktu yang telah diedit: April 19, 2024, 16:00 UTC

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

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "OrganizationsPolicies",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DescribeOrgAccounts",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount"
      ],
      "Resource" : [
        "arn:aws:organizations::*:account/o-*/*"
      ]
    },
    {
      "Sid" : "AllowManagementOfServiceLinkedChannel",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateServiceLinkedChannel",
```

```
        "cloudtrail:DeleteServiceLinkedChannel",
        "cloudtrail:GetServiceLinkedChannel",
        "cloudtrail:UpdateServiceLinkedChannel"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:channel/aws-service-channel/security-lake/*"
    },
    {
      "Sid" : "AllowListServiceLinkedChannel",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:ListServiceLinkedChannels"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeAnyVpc",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListDelegatedAdmins",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowWafLoggingConfiguration",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:PutLoggingConfiguration",
        "wafv2:GetLoggingConfiguration",
        "wafv2:ListLoggingConfigurations",
        "wafv2:DeleteLoggingConfiguration"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "wafv2:LogScope" : "SecurityLake"
        }
      }
    },
    {
      "Sid" : "AllowPutLoggingConfiguration",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:PutLoggingConfiguration"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "wafv2:LogDestinationResource" : "arn:aws:s3:::aws-waf-logs-security-lake-*"
        }
      }
    },
    {
      "Sid" : "ListWebACLs",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:ListWebACLs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LogDelivery",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:DeleteLogDelivery"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "wafv2.amazonaws.com"
          ]
        }
      }
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

ServerMigration_ServiceRole

Deskripsi: Izin untuk mengizinkan Layanan Migrasi AWS Server bermigrasi VMs ke EC2: memungkinkan Layanan Migrasi Server menempatkan sumber daya yang dimigrasi ke akun pelanggan. EC2

`ServerMigration_ServiceRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ServerMigration_ServiceRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 11 Agustus 2020 20:41 UTC
- Waktu yang telah diedit: 15 Oktober 2020, 17:26 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ServerMigration_ServiceRole`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:CreateStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/sms-app-*/*",
      "Condition" : {
        "Null" : {
          "cloudformation:ResourceTypes" : "false"
        },
        "ForAllValues:StringEquals" : {
          "cloudformation:ResourceTypes" : [
            "AWS::EC2::Instance",
            "AWS::ApplicationInsights::Application",
            "AWS::ResourceGroups::Group"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DeleteStack",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources",
        "cloudformation:GetTemplate"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/sms-app-*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ValidateTemplate",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteObject",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:PutLifecycleConfiguration"
      ],
      "Resource" : "arn:aws:s3:::sms-app-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sms:CreateReplicationJob",
        "sms:DeleteReplicationJob",
        "sms:GetReplicationJobs",
        "sms:GetReplicationRuns",
        "sms:GetServers",
        "sms:ImportServerCatalog",
        "sms:StartOnDemandReplicationRun",
        "sms:UpdateReplicationJob"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ssm:*::document/AWS-RunRemoteScript",
        "arn:aws:s3:::sms-app-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
```

```
        "StringEquals" : {
          "ssm:resourceTag/UseForSMSApplicationValidation" : [
            "true"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CancelCommand",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CopySnapshot"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CopySnapshot",
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/SMSJobId" : [
            "sms-*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotAttribute",
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
```

```
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/SMSJobId" : [
            "sms-*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopyImage",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSnapshotAttribute",
        "ec2:DeregisterImage",
        "ec2:ImportImage",
        "ec2:DescribeImportImageTasks",
        "ec2:GetEbsEncryptionByDefault"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetInstanceProfile"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DisassociateIamInstanceProfile",
        "ec2:AssociateIamInstanceProfile",
        "ec2:ReplaceIamInstanceProfileAssociation"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/sms-app-*/*"
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "iam:PassedToService" : "cloudformation.amazonaws.com"
        },
        "StringLike" : {
          "iam:AssociatedResourceArn" : "arn:aws:cloudformation:*:*:stack/sms-app-*/*"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

ServerMigrationConnector

Deskripsi: Izin untuk mengizinkan Konektor Migrasi AWS Server bermigrasi VMs ke. EC2 Memungkinkan komunikasi dengan Layanan Migrasi AWS Server, akses baca/tulis ke bucket S3 dimulai dengan 'sms-b-' dan 'import-to-ec2-' serta bucket yang digunakan untuk peningkatan

Konektor Migrasi AWS Server, pendaftaran Konektor Migrasi Server dengan, dan metrik yang AWS diunggah ke. AWS AWS

`ServerMigrationConnector`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ServerMigrationConnector` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 24 Oktober 2016, 21:45 UTC
- Waktu telah diedit: 24 Oktober 2016, 21:45 UTC
- ARN: `arn:aws:iam::aws:policy/ServerMigrationConnector`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:GetUser",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sms:SendMessage",
        "sms:GetMessages"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteObject",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:PutLifecycleConfiguration",
        "s3:AbortMultipartUpload",
        "s3:ListBucketMultipartUploads",
        "s3:ListMultipartUploadParts"
      ],
      "Resource" : [
        "arn:aws:s3:::sms-b-*",
        "arn:aws:s3:::import-to-ec2-*",
        "arn:aws:s3:::server-migration-service-upgrade",
        "arn:aws:s3:::server-migration-service-upgrade/*",
        "arn:aws:s3:::connector-platform-upgrade-info/*",
        "arn:aws:s3:::connector-platform-upgrade-info",
        "arn:aws:s3:::connector-platform-upgrade-bundles/*",
        "arn:aws:s3:::connector-platform-upgrade-bundles",
        "arn:aws:s3:::connector-platform-release-notes/*",
        "arn:aws:s3:::connector-platform-release-notes"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "awsconnector:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "SNS:Publish"
      ],
      "Resource" : "arn:aws:sns:*:*:metrics-sns-topic-for-*"
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

ServerMigrationServiceConsoleFullAccess

Deskripsi: Izin yang diperlukan untuk menggunakan semua fitur Konsol Layanan Migrasi Server

`ServerMigrationServiceConsoleFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ServerMigrationServiceConsoleFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 09 Mei 2020, 17:18 UTC
- Waktu yang telah diedit: 20 Juli 2020, 22:00 UTC
- ARN: `arn:aws:iam::aws:policy/ServerMigrationServiceConsoleFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "sms:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "cloudformation:ListStacks",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackResources"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : "s3:ListAllMyBuckets",
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::sms-app-*/*"
    },
    {
      "Action" : [
        "ec2:DescribeKeyPairs",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
```

```
        "iam:ListRoles"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "sms.amazonaws.com"
        }
      },
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:GetInstanceProfile",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

ServerMigrationServiceLaunchRole

Deskripsi: Izin untuk mengizinkan Layanan Migrasi AWS Server membuat dan memperbarui AWS sumber daya yang relevan ke pelanggan Akun AWS untuk meluncurkan server dan aplikasi yang dimigrasi.

`ServerMigrationServiceLaunchRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ServerMigrationServiceLaunchRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 26 November 2018, 19:53 UTC
- Waktu yang telah diedit: 15 Oktober 2020, 17:29 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ServerMigrationServiceLaunchRole`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyInstanceAttribute",
        "ec2:StopInstances",
        "ec2:StartInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
 "arn:aws:cloudformation:*:*:stack/sms-app-*/*"
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DisassociateIamInstanceProfile",
        "ec2:AssociateIamInstanceProfile",
        "ec2:ReplaceIamInstanceProfileAssociation"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/sms-app-*/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "applicationinsights:Describe*",
```

```
        "applicationinsights:List*",
        "cloudformation:ListStackResources",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "applicationinsights:CreateApplication",
        "applicationinsights:CreateComponent",
        "applicationinsights:UpdateApplication",
        "applicationinsights:DeleteApplication",
        "applicationinsights:UpdateComponentConfiguration",
        "applicationinsights:DeleteComponent"
      ],
      "Resource" : "arn:aws:applicationinsights:*:*:application/resource-group/sms-app-
*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:GetGroup",
        "resource-groups:UpdateGroup",
        "resource-groups:DeleteGroup"
      ],
      "Resource" : "arn:aws:resource-groups:*:*:group/sms-app-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/aws:cloudformation:stack-id" :
 "arn:aws:cloudformation:*:*:stack/sms-app-*/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/application-insights.amazonaws.com/
AWSServiceRoleForApplicationInsights"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "application-insights.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

ServerMigrationServiceRoleForInstanceValidation

Deskripsi: Izin untuk memungkinkan AWS SMS menjalankan skrip validasi data yang digunakan dan mengirim skrip keberhasilan/kegagalan kembali ke SMS

`ServerMigrationServiceRoleForInstanceValidation`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ServerMigrationServiceRoleForInstanceValidation` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 20 Juli 2020, 22:25 UTC
- Waktu yang telah diedit: 20 Juli 2020, 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ServerMigrationServiceRoleForInstanceValidation`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::sms-app-*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "sms:NotifyAppValidationOutput",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

ServiceQuotasFullAccess

Deskripsi: Menyediakan akses penuh ke Service Quotas

`ServiceQuotasFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ServiceQuotasFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 24 Juni 2019, 15:44 UTC
- Waktu yang telah diedit: 04 Februari 2021, 21:29 UTC
- ARN: `arn:aws:iam::aws:policy/ServiceQuotasFullAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAccountLimits",
        "cloudformation:DescribeAccountLimits",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:PutMetricAlarm",
        "dynamodb:DescribeLimits",
        "elasticloadbalancing:DescribeAccountLimits",
        "iam:GetAccountSummary",
        "kinesis:DescribeLimits",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
```

```
        "organizations:ListAWSServiceAccessForOrganization",
        "rds:DescribeAccountAttributes",
        "route53:GetAccountLimit",
        "tag:GetTagKeys",
        "tag:GetTagValues",
        "servicequotas:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/ServiceQuotaMonitor" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "organizations:ServicePrincipal" : [
            "servicequotas.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "servicequotas.amazonaws.com"
```

```
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

ServiceQuotasReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Service Quotas

`ServiceQuotasReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ServiceQuotasReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 24 Juni 2019, 15:31 UTC
- Waktu yang telah diedit: 21 Desember 2020, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/ServiceQuotasReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAccountLimits",
        "cloudformation:DescribeAccountLimits",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "dynamodb:DescribeLimits",
        "elasticloadbalancing:DescribeAccountLimits",
        "iam:GetAccountSummary",
        "kinesis:DescribeLimits",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "rds:DescribeAccountAttributes",
        "route53:GetAccountLimit",
        "tag:GetTagKeys",
        "tag:GetTagValues",
        "servicequotas:GetAssociationForServiceQuotaTemplate",
        "servicequotas:GetAWSDefaultServiceQuota",
        "servicequotas:GetRequestedServiceQuotaChange",
        "servicequotas:GetServiceQuota",
        "servicequotas:GetServiceQuotaIncreaseRequestFromTemplate",
        "servicequotas:ListAWSDefaultServiceQuotas",
        "servicequotas:ListRequestedServiceQuotaChangeHistory",
        "servicequotas:ListRequestedServiceQuotaChangeHistoryByQuota",
        "servicequotas:ListServices",
        "servicequotas:ListServiceQuotas",
        "servicequotas:ListServiceQuotaIncreaseRequestsInTemplate",
        "servicequotas:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

ServiceQuotasServiceRolePolicy

Deskripsi: Memungkinkan Service Quotas untuk membuat kasus dukungan atas nama Anda

`ServiceQuotasServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 22 Mei 2019, 20:44 UTC
- Waktu yang telah diedit: 24 Juni 2019, 14:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ServiceQuotasServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

SimpleWorkflowFullAccess

Deskripsi: Menyediakan akses penuh ke layanan konfigurasi Alur Kerja Sederhana.

`SimpleWorkflowFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `SimpleWorkflowFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu telah diedit: 06 Februari 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/SimpleWorkflowFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

SMSVoiceServiceRolePolicy

Deskripsi: Memungkinkan SMSVoice untuk mempublikasikan metrik CloudWatch atas nama Anda

`SMSVoiceServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 14 November 2024, 17:04 UTC
- Waktu yang telah diedit: 14 November 2024, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/SMSVoiceServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

SplitCostAllocationDataServiceRolePolicy

Deskripsi: Memungkinkan data alokasi biaya terpisah untuk mengambil informasi AWS Organizations, jika berlaku, dan mengumpulkan data telemetri untuk layanan data alokasi biaya terpisah yang telah dipilih pelanggan.

`SplitCostAllocationDataServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 16 April 2024, 16:05 UTC
- Waktu yang telah diedit: 16 April 2024, 16:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/SplitCostAllocationDataServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

SSMQuickSetupRolePolicy

Deskripsi: Memberikan izin untuk memeriksa kesehatan konfigurasi Pengaturan Cepat, memastikan penggunaan parameter dan sumber daya yang disediakan secara konsisten, dan memulihkan sumber daya saat drift terdeteksi.

`SSMQuickSetupRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 25 Juni 2024, 15:20 UTC
- Waktu telah diedit: November 18, 2024, 13:06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/SSMQuickSetupRolePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

SupportUser

Deskripsi: Kebijakan ini memberikan izin untuk memecahkan masalah dan menyelesaikan masalah dalam file. Akun AWS Kebijakan ini juga memungkinkan pengguna untuk menghubungi AWS dukungan untuk membuat dan mengelola kasus.

`SupportUser`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `SupportUser` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan fungsi Job
- Waktu pembuatan: 10 November 2016, 17:21 UTC
- Waktu telah diedit: Agustus 25, 2023, 18:40 UTC

- ARN: `arn:aws:iam::aws:policy/job-function/SupportUser`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "support:*",
        "acm:DescribeCertificate",
        "acm:GetCertificate",
        "acm:List*",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:ListCertificateAuthorities",
        "apigateway:GET",
        "autoscaling:Describe*",
        "aws-marketplace:ViewSubscriptions",
        "cloudformation:Describe*",
        "cloudformation:Get*",
        "cloudformation:List*",
        "cloudformation:EstimateTemplateCost",
        "cloudfront:Get*",
        "cloudfront:List*",
        "cloudsearch:Describe*",
        "cloudsearch:List*",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:LookupEvents",
        "cloudtrail:ListTags",
        "cloudtrail:ListPublicKeys",
        "cloudwatch:Describe*",
        "cloudwatch:Get*",
        "cloudwatch:List*",
```

```
        "codecommit:BatchGetRepositories",
        "codecommit:Get*",
        "codecommit:List*",
        "codedeploy:Batch*",
        "codedeploy:Get*",
        "codedeploy:List*",
        "codepipeline:AcknowledgeJob",
        "codepipeline:AcknowledgeThirdPartyJob",
        "codepipeline:ListActionTypes",
        "codepipeline:ListPipelines",
        "codepipeline:PollForJobs",
        "codepipeline:PollForThirdPartyJobs",
        "codepipeline:GetPipelineState",
        "codepipeline:GetPipeline",
        "cognito-identity:List*",
        "cognito-identity:LookupDeveloperIdentity",
        "cognito-identity:Describe*",
        "cognito-idp:DescribeResourceServer",
        "cognito-idp:DescribeRiskConfiguration",
        "cognito-idp:DescribeUserImportJob",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolDomain",
        "cognito-idp:List*",
        "cognito-sync:Describe*",
        "cognito-sync:GetBulkPublishDetails",
        "cognito-sync:GetCognitoEvents",
        "cognito-sync:GetIdentityPoolConfiguration",
        "cognito-sync:List*",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:DescribeConfigRuleEvaluationStatus",
        "config:DescribeConfigRules",
        "config:DescribeDeliveryChannels",
        "config:DescribeDeliveryChannelStatus",
        "config:GetResourceConfigHistory",
        "config:ListDiscoveredResources",
        "datapipeline:DescribeObjects",
        "datapipeline:DescribePipelines",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:ListPipelines",
        "datapipeline:QueryObjects",
        "datapipeline:ReportTaskProgress",
        "datapipeline:ReportTaskRunnerHeartbeat",
        "devicefarm:List*",
```

```
        "devicefarm:Get*",
        "directconnect:Describe*",
        "discovery:Describe*",
        "discovery:ListConfigurations",
        "dms:Describe*",
        "dms:List*",
        "ds:DescribeDirectories",
        "ds:DescribeSnapshots",
        "ds:GetDirectoryLimits",
        "ds:GetSnapshotLimits",
        "ds:ListAuthorizedApplications",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeTable",
        "dynamodb:ListTables",
        "ec2:Describe*",
        "ec2:DescribeHosts",
        "ec2:describeIdentityIdFormat",
        "ec2:DescribeIdFormat",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeNatGateways",
        "ec2:DescribeReservedInstancesModifications",
        "ec2:DescribeTags",
        "ec2:SearchLocalGatewayRoutes",
        "ecr:GetRepositoryPolicy",
        "ecr:BatchCheckLayerAvailability",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "ecs:Describe*",
        "ecs:List*",
        "elasticache:Describe*",
        "elasticache:List*",
        "elasticbeanstalk:Check*",
        "elasticbeanstalk:Describe*",
        "elasticbeanstalk:List*",
        "elasticbeanstalk:RequestEnvironmentInfo",
        "elasticbeanstalk:RetrieveEnvironmentInfo",
        "elasticbeanstalk:ValidateConfigurationSettings",
        "elasticfilesystem:Describe*",
        "elasticloadbalancing:Describe*",
        "elasticmapreduce:Describe*",
        "elasticmapreduce:List*",
        "elastictranscoder:List*",
        "elastictranscoder:ReadJob",
        "elasticfilesystem:DescribeFileSystems",
```

```
        "es:Describe*",
        "es:List*",
        "es:ESHttpGet",
        "es:ESHttpHead",
        "events:DescribeRule",
        "events:List*",
        "events:TestEventPattern",
        "firehose:Describe*",
        "firehose:List*",
        "gamelift:List*",
        "gamelift:Describe*",
        "glacier:ListVaults",
        "glacier:DescribeVault",
        "glacier:DescribeJob",
        "glacier:Get*",
        "glacier:List*",
        "iam:GenerateCredentialReport",
        "iam:GenerateServiceLastAccessedDetails",
        "iam:Get*",
        "iam:List*",
        "importexport:GetStatus",
        "importexport:ListJobs",
        "inspector:Describe*",
        "inspector:List*",
        "iot:Describe*",
        "iot:Get*",
        "iot:List*",
        "kinesisanalytics:DescribeApplication",
        "kinesisanalytics:DiscoverInputSchema",
        "kinesisanalytics:GetApplicationState",
        "kinesisanalytics:ListApplications",
        "kinesis:Describe*",
        "kinesis:Get*",
        "kinesis:List*",
        "kms:Describe*",
        "kms:Get*",
        "kms:List*",
        "lambda:List*",
        "lambda:Get*",
        "logs:Describe*",
        "logs:TestMetricFilter",
        "machinelearning:Describe*",
        "machinelearning:Get*",
        "opsworks:Describe*",
```

```
        "rds:Describe*",
        "rds:ListTagsForResource",
        "redshift:Describe*",
        "route53:Get*",
        "route53:List*",
        "route53domains:CheckDomainAvailability",
        "route53domains:GetDomainDetail",
        "route53domains:GetOperationDetail",
        "route53domains:List*",
        "s3:List*",
        "sdb:GetAttributes",
        "sdb:List*",
        "sdb:Select*",
        "servicecatalog:SearchProducts",
        "servicecatalog:DescribeProduct",
        "servicecatalog:DescribeProductView",
        "servicecatalog:ListLaunchPaths",
        "servicecatalog:DescribeProvisioningParameters",
        "servicecatalog:ListRecordHistory",
        "servicecatalog:DescribeRecord",
        "servicecatalog:ScanProvisionedProducts",
        "ses:Get*",
        "ses:List*",
        "sns:Get*",
        "sns:List*",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ListQueues",
        "sqs:ReceiveMessage",
        "ssm:List*",
        "ssm:Describe*",
        "storagegateway:Describe*",
        "storagegateway:List*",
        "swf:Count*",
        "swf:Describe*",
        "swf:Get*",
        "swf:List*",
        "waf:Get*",
        "waf:List*",
        "workdocs:Describe*",
        "workmail:Describe*",
        "workmail:Get*",
        "workspaces:Describe*"
      ],
```

```
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

SystemAdministrator

Deskripsi: Memberikan izin akses penuh yang diperlukan untuk sumber daya yang diperlukan untuk operasi aplikasi dan pengembangan.

`SystemAdministrator`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `SystemAdministrator` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan fungsi Job
- Waktu pembuatan: 10 November 2016, 17:23 UTC
- Waktu yang telah diedit: 11 Februari 2025, 22:07 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/SystemAdministrator`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Statement" : [
    {
      "Action" : [
        "acm:Describe*",
        "acm:Get*",
        "acm:List*",
        "acm:Request*",
        "acm:Resend*",
        "autoscaling:*",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:ListPublicKeys",
        "cloudtrail:ListTags",
        "cloudtrail:LookupEvents",
        "cloudtrail:StartLogging",
        "cloudtrail:StopLogging",
        "cloudwatch:*",
        "codecommit:BatchGetRepositories",
        "codecommit:CreateBranch",
        "codecommit:CreateRepository",
        "codecommit:Get*",
        "codecommit:GitPull",
        "codecommit:GitPush",
        "codecommit:List*",
        "codecommit:Put*",
        "codecommit:Test*",
        "codecommit:Update*",
        "codedeploy:*",
        "codepipeline:*",
        "config:*",
        "ds:*",
        "ec2:Allocate*",
        "ec2:AssignPrivateIpAddresses*",
        "ec2:Associate*",
        "ec2:Allocate*",
        "ec2:AttachInternetGateway",
        "ec2:AttachNetworkInterface",
        "ec2:AttachVpnGateway",
        "ec2:Bundle*",
        "ec2:Cancel*",
```

```
        "ec2:Copy*",
        "ec2:CreateCustomerGateway",
        "ec2:CreateDhcpOptions",
        "ec2:CreateFlowLogs",
        "ec2:CreateImage",
        "ec2:CreateInstanceExportTask",
        "ec2:CreateInternetGateway",
        "ec2:CreateKeyPair",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion",
        "ec2:CreateNatGateway",
        "ec2:CreateNetworkInterface",
        "ec2:CreatePlacementGroup",
        "ec2:CreateReservedInstancesListing",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSnapshot",
        "ec2:CreateSpotDatafeedSubscription",
        "ec2:CreateSubnet",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:CreateVpc",
        "ec2:CreateVpcEndpoint",
        "ec2:CreateVpnConnection",
        "ec2:CreateVpnConnectionRoute",
        "ec2:CreateVpnGateway",
        "ec2:DeleteFlowLogs",
        "ec2:DeleteKeyPair",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions",
        "ec2:DeleteNatGateway",
        "ec2:DeleteNetworkInterface",
        "ec2:DeletePlacementGroup",
        "ec2:DeleteSnapshot",
        "ec2:DeleteSpotDatafeedSubscription",
        "ec2:DeleteSubnet",
        "ec2:DeleteTags",
        "ec2:DeleteVpc",
        "ec2:DeleteVpcEndpoints",
        "ec2:DeleteVpnConnection",
        "ec2:DeleteVpnConnectionRoute",
        "ec2:DeleteVpnGateway",
        "ec2:DeregisterImage",
```

```
        "ec2:Describe*",
        "ec2:DetachInternetGateway",
        "ec2:DetachNetworkInterface",
        "ec2:DetachVpnGateway",
        "ec2:DisableVgwRoutePropagation",
        "ec2:DisableVpcClassicLinkDnsSupport",
        "ec2:DisassociateAddress",
        "ec2:DisassociateRouteTable",
        "ec2:EnableVgwRoutePropagation",
        "ec2:EnableVolumeIO",
        "ec2:EnableVpcClassicLinkDnsSupport",
        "ec2:GetConsoleOutput",
        "ec2:GetHostReservationPurchasePreview",
        "ec2:GetLaunchTemplateData",
        "ec2:GetPasswordData",
        "ec2: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",
        "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"
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

TranslateFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Translate.

`TranslateFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `TranslateFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 November 2018, 23:36 UTC
- Waktu yang telah diedit: 08 Januari 2020, 21:22 UTC
- ARN: `arn:aws:iam::aws:policy/TranslateFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

```
      "Action" : [
        "translate:*",
        "comprehend:DetectDominantLanguage",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "iam:ListRoles",
        "iam:GetRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

TranslateReadOnly

Deskripsi: Menyediakan akses hanya-baca ke Amazon Translate.

`TranslateReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `TranslateReadOnly` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 November 2017, 18:22 UTC
- Waktu yang telah diedit: 24 Mei 2023, 17:19 UTC

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

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "translate:TranslateText",
        "translate:TranslateDocument",
        "translate:GetTerminology",
        "translate:ListTerminologies",
        "translate:ListTextTranslationJobs",
        "translate:DescribeTextTranslationJob",
        "translate:GetParallelData",
        "translate:ListParallelData",
        "comprehend:DetectDominantLanguage",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

ViewOnlyAccess

Deskripsi: Kebijakan ini memberikan izin untuk melihat sumber daya dan metadata dasar di semua layanan. AWS

`ViewOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ViewOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan fungsi Job
- Waktu pembuatan: 10 November 2016, 17:20 UTC
- Waktu yang telah diedit: 28 Mei 2025, 16:22 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/ViewOnlyAccess`

Versi kebijakan

Versi kebijakan: v25 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

VMImportExportRoleForAWSConnector

Deskripsi: Kebijakan default untuk peran layanan Impor/Ekspor VM, untuk pelanggan yang menggunakan Konektor. AWS Layanan Impor/Ekspor VM berperan dalam kebijakan ini untuk memenuhi permintaan migrasi mesin virtual dari alat virtual Connector. AWS (Perhatikan bahwa AWS Konektor menggunakan kebijakan terkelola AWSConnector "" untuk mengeluarkan permintaan atas nama pelanggan ke layanan Impor/Ekspor VM.) Menyediakan kemampuan untuk membuat AMIs dan

EBS snapshot, memodifikasi atribut snapshot EBS, membuat panggilan “Describe*” pada EC2 objek, dan membaca dari bucket S3 dimulai dengan '2-'. import-to-ec

`VMImportExportRoleForAWSConnector`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `VMImportExportRoleForAWSConnector` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 03 September 2015, 20:48 UTC
- Waktu telah diedit: 03 September 2015, 20:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/VMImportExportRoleForAWSConnector`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:GetObject"
      ],
      "Resource" : [
```

```
        "arn:aws:s3:::import-to-ec2-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotAttribute",
        "ec2:CopySnapshot",
        "ec2:RegisterImage",
        "ec2:Describe*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

VPCLatticeFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon VPC Lattice dan akses ke layanan ketergantungan.

`VPCLatticeFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `VPCLatticeFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 Maret 2023, 02:49 UTC
- Waktu yang telah diedit: 01 Desember 2024, 14:21 UTC
- ARN: `arn:aws:iam::aws:policy/VPCLatticeFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:*",
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:DescribeLoadBalancers",
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams",
        "logs:DescribeLogGroups",
        "s3:ListAllMyBuckets",
        "lambda:ListAliases",
        "lambda:ListFunctions",
        "lambda:ListVersionsByFunction",
        "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"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

VPCLatticeReadOnlyAccess

Deskripsi: Menyediakan akses hanya-baca ke Amazon VPC Lattice melalui AWS Management Console, dan akses terbatas ke layanan dependensi.

`VPCLatticeReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `VPCLatticeReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 Maret 2023, 02:47 UTC
- Waktu yang telah diedit: 01 Desember 2024, 14:21 UTC
- ARN: `arn:aws:iam::aws:policy/VPCLatticeReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:Get*",
        "vpc-lattice:List*",
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "cloudwatch:GetMetricData",
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:DescribeLoadBalancers",
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams",
        "lambda:ListAliases",
        "lambda:ListFunctions",
        "lambda:ListVersionsByFunction",
        "logs:DescribeLogGroups",
        "logs:GetLogDelivery",
        "logs:ListLogDeliveries",
        "s3:ListAllMyBuckets",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

VPCLatticeServicesInvokeAccess

Deskripsi: Menyediakan akses untuk menjalankan layanan Amazon VPC Lattice.

`VPCLatticeServicesInvokeAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `VPCLatticeServicesInvokeAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 Maret 2023, 02:45 UTC
- Waktu yang telah diedit: 30 Maret 2023, 02:45 UTC
- ARN: `arn:aws:iam::aws:policy/VPCLatticeServicesInvokeAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice-svcs:Invoke"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

WAFLoggingServiceRolePolicy

Deskripsi: Membuat SLR untuk menulis log pelanggan ke aliran firehose

`WAFLoggingServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 24 Agustus 2018, 21:05 UTC
- Waktu telah diedit: 24 Agustus 2018, 21:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/WAFLoggingServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : [
        "arn:aws:firehose:*:*:deliverystream/aws-waf-logs-*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

WAFRegionalLoggingServiceRolePolicy

Deskripsi: Membuat SLR untuk menulis log pelanggan ke aliran firehose

`WAFRegionalLoggingServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 24 Agustus 2018, 18:40 UTC

- Waktu telah diedit: 24 Agustus 2018, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/WAFRegionalLoggingServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : [
        "arn:aws:firehose:*:*:deliverystream/aws-waf-logs-*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

WAFV2LoggingServiceRolePolicy

Deskripsi: Kebijakan ini membuat peran terkait layanan yang memungkinkan AWS WAF menulis log ke Amazon Kinesis Data Firehose.

`WAFV2LoggingServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 07 November 2019 00:40 UTC
- Waktu yang telah diedit: 03 Juni 2024, 17:29 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/WAFV2LoggingServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

WellArchitectedConsoleFullAccess

Deskripsi: Menyediakan akses penuh ke AWS Well-Architected Tool melalui AWS Management Console

`WellArchitectedConsoleFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `WellArchitectedConsoleFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 November 2018, 18:19 UTC
- Waktu telah diedit: 29 November 2018, 18:19 UTC
- ARN: `arn:aws:iam::aws:policy/WellArchitectedConsoleFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

WellArchitectedConsoleReadOnlyAccess

Deskripsi: Menyediakan akses read-only ke Well-Architected AWS Tool melalui AWS Management Console

`WellArchitectedConsoleReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `WellArchitectedConsoleReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 November 2018, 18:21 UTC
- Waktu yang telah diedit: 29 Juni 2023, 17:16 UTC
- ARN: `arn:aws:iam::aws:policy/WellArchitectedConsoleReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

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

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

WorkLinkServiceRolePolicy

Deskripsi: Mengaktifkan akses ke Layanan AWS dan Sumber Daya yang digunakan atau dikelola oleh Amazon WorkLink

`WorkLinkServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `WorkLinkServiceRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 23 Januari 2019, 19:03 UTC
- Waktu yang telah diedit: 23 Januari 2019, 19:03 UTC
- ARN: `arn:aws:iam::aws:policy/WorkLinkServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:PutRecord",
        "kinesis:PutRecords"
      ],
      "Resource" : "arn:aws:kinesis:*:*:stream/AmazonWorkLink-*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.